

**Development of an intelligent e-commerce  
assurance model to promote trust in online  
shopping environments**

by

**Thembekile Olivia Mayayise**

Submitted in accordance with the requirements for the degree of

**DOCTOR OF PHILOSOPHY**

in the subject of

**INFORMATION SYSTEMS**

at the

School of Computing, College of Science, Engineering and  
Technology,

**UNIVERSITY OF SOUTH AFRICA**

SUPERVISOR: Professor Isaac O. Osunmakinde

January 2018

# DECLARATION

**Student number: 33070679**

I declare that “**Development of an intelligent e-commerce assurance model to promote trust in online shopping environments**” is my own work and that I have referenced and acknowledged all the sources that I have used by means of complete references.

I further declare that I submitted the thesis to originality checking software. The result summary is attached.

I further declare that I have not previously submitted this work or part of it for examination at UNISA for another qualification or at any other higher education institution.

---

**Signature**

Thembekile Olivia Mayayise

---

**Date**

# **DEDICATION**

I dedicate my PhD to my siblings (Vernon, Phumzile and Puxley), parents, my mother, Madeleine Mashao, and my late father, Prince Mashao. A special note of gratitude to my husband (Kulani) and our children (Ndzalo and Sagwadi) for their unwavering support throughout this journey. To God Almighty for making it possible by His Grace.

# ACKNOWLEDGEMENTS

When I enrolled for this PhD degree, I was faced with a great many uncertainties and I was not sure if I would complete the degree, considering my other roles and responsibilities as a wife and mother, among others.

In retrospect, completing my degree at UNISA has been a blessing, considering the amount of resources and assistance UNISA provides to its students who are pursuing post-graduate degrees. I still remember attending a seminar, which was arranged by UNISA and conducted by Dr Erik Hofste, on writing good dissertations. This was one of many sources of support that the institution made available to assist me and fellow students to conduct research and for that I am very grateful.

I would like to acknowledge and thank my supervisor, Professor Isaac Olusegun Osunmakinde, for his unfailing support and supervision. Through his guidance and teaching I have learnt to write good academic papers and to make presentations at academic conferences. He instilled so much confidence in me as a student and imparted so much knowledge that I am in awe of his generosity and skills. Professor Osunmakinde was very straightforward and with all his reviews I always knew where I stood, which helped me a lot to stay focused. Professor Osunmakinde is very honest and sets very high standards for his students and I will always be grateful for his dedication, support, availability and guidance throughout. His ability always to see the end from the beginning inspired me, as did his style of teaching and supervision.

My husband, Kulani, and our children, Ndzalo and Sagwadi, have been my pillars of support throughout this entire journey. To my cheerleaders: My mom (Madelaine Mashao) and my sister (Phumzile Arko-Cobbah), your motivation has come a long way in seeing me through the completion of this degree.

Lastly, I believe that it is by God's grace that I have gone through this journey until the end. To Him be the Glory!

# ABSTRACT

Electronic commerce (e-commerce) markets provide benefits for both buyers and sellers; however, because of cyber security risks consumers are reluctant to transact online. Trust in e-commerce is paramount for adoption. Trust as a subject for research has been a term considered in depth by numerous researchers in various fields of study, including psychology and information technology. Various models have been developed in e-commerce to alleviate consumer fears, thus promoting trust in online environments. Third-party web seals and online scanning tools are some of the existing models used in e-commerce environments, but they have some deficiencies, e.g. failure to incorporate compliance, which need to be addressed.

This research proposes an e-commerce assurance model for safe online shopping. The machine learning model is called the Page ranking analytical hierarchy process (PRAHP). PRAHP builds complementary strengths of the analytical hierarchy process (AHP) and Page ranking (PR) techniques to evaluate the trustworthiness of web attributes. The attributes that are assessed are Adaptive legislation, Adaptive International Organisation for Standardisation Standards, Availability, Policy and Advanced Security login. The attributes were selected based on the literature reviewed from accredited journals and some of the reputable e-commerce websites.

PRAHP's paradigms were evaluated extensively through detailed experiments on business-to-business, business-to-consumer, cloud-based and general e-commerce websites. The results of the assessments were validated by customer inputs regarding the website. The reliability and robustness of PRAHP was tested by varying the damping factor and the inbound links. In all the experiments, the results revealed that the model provides reliable results to guide customers in making informed purchasing decisions. The research also reveals hidden e-commerce topics that have not received attention, which generates knowledge and opens research questions for future researchers. These ultimately made significant contributions in e-commerce assurance, in areas such as security and compliance through the fusing of AHP and PR, integrated into a decision table for alleviating trustworthiness anxiety in various e-commerce transacting partners, e-commerce platforms and markets.

**Key words:** *E-commerce, Assurance, AHP, Page rank, Security, Policy, Compliance, Trust*

# TABLE OF CONTENTS

<b>DECLARATION.....</b>	<b>i</b>
<b>DEDICATION.....</b>	<b>ii</b>
<b>ACKNOWLEDGEMENTS .....</b>	<b>iii</b>
<b>ABSTRACT .....</b>	<b>iv</b>
<b>TABLE OF CONTENTS .....</b>	<b>v</b>
<b>LIST OF FIGURES .....</b>	<b>ix</b>
<b>LIST OF TABLES .....</b>	<b>x</b>
<b>LIST OF ABBREVIATIONS .....</b>	<b>xi</b>
<b>CHAPTER 1: INTRODUCTION.....</b>	<b>1</b>
<b>1.1 BACKGROUND .....</b>	<b>1</b>
<b>1.2 PROBLEM STATEMENT .....</b>	<b>4</b>
<b>1.3 RESEARCH OBJECTIVES .....</b>	<b>6</b>
<b>1.4 RESEARCH QUESTIONS.....</b>	<b>7</b>
<b>1.5 RESEARCH DESIGN.....</b>	<b>8</b>
<b>1.6 RESEARCH CONTRIBUTIONS .....</b>	<b>10</b>
1.6.1 Contributions to the scientific body of knowledge .....	10
1.6.2 Declaration of publications resulting from this study .....	10
<b>1.7 RESEARCH ETHICAL CONSIDERATIONS.....</b>	<b>11</b>
<b>1.8 SCOPE AND CONTEXT OF THE STUDY .....</b>	<b>12</b>
1.8.1 Research scope.....	12
1.8.2 Research limitations.....	12
<b>1.9 RESEARCH SYNOPSIS.....</b>	<b>13</b>
<b>1.10 CHAPTER SUMMARY .....</b>	<b>14</b>
<b>CHAPTER 2: LITERATURE SURVEY AND THEORETICAL BACKGROUND .....</b>	<b>15</b>
<b>2.1 PRELIMINARIES.....</b>	<b>15</b>
<b>2.2 E-COMMERCE ASSURANCE MODELS AND TRUSTWORTHINESS ISSUES .....</b>	<b>15</b>
2.2.1 Trustworthiness fears .....	15
2.2.2 E-commerce assurance model paradigms .....	19
2.2.3 Cloud-based assurance models in e-commerce.....	20
2.2.4 E-commerce applications .....	22
2.2.5 Third-party seal assurances.....	23
2.2.6 Investigation of weaknesses of third-party assurance methods .....	33

2.2.7 Important attributes of e-commerce assurance models .....	35
2.2.8 Comparative evaluations of e-commerce assurance models.....	36
2.2.9 Gaps identified in the literature.....	37
<b>2.3 POPULAR AREAS OF E-COMMERCE ASSURANCE .....</b>	<b>38</b>
2.3.1 Business-to-consumer assurance.....	38
2.3.2 Business-to-business assurance.....	38
2.3.3 Cloud-based assurance .....	39
2.3.4 Consumer-to-consumer assurance .....	40
2.3.5 Mobile e-commerce assurance.....	40
<b>2.4 BUSINESS-TO-CONSUMER ASSURANCE .....</b>	<b>41</b>
2.4.1 Business-to-consumer assurance background.....	41
2.4.2 Business-to-consumer e-commerce risks .....	43
2.4.3 Business-to-consumer assurance model challenges.....	45
2.4.4 Comparisons of various B2C assurance models .....	46
<b>2.5 BUSINESS-TO-BUSINESS ASSURANCE .....</b>	<b>50</b>
2.5.1 Business-to-business assurance background.....	50
2.5.2 Business-to-business e-commerce risks .....	52
2.5.3 Business-to-business assurance model challenges.....	53
2.5.4 Comparisons of various B2B assurance models .....	54
<b>2.6 CLOUD-BASED E-COMMERCE ASSURANCE.....</b>	<b>54</b>
2.6.1 Cloud computing background .....	54
2.6.2 Cloud e-commerce risks.....	56
2.6.3 Cloud assurance methods challenges .....	59
2.6.4 Comparisons of cloud assurance models .....	64
<b>2.7 SELECTED MACHINE LEARNING THEORIES .....</b>	<b>64</b>
2.7.1 Page ranking.....	64
2.7.2 Analytical hierarchy process .....	67
<b>2.8 CHAPTER SUMMARY .....</b>	<b>72</b>
<b>CHAPTER 3: RESEARCH DESIGN AND METHODOLOGY.....</b>	<b>73</b>
<b>3.1 INTRODUCTION.....</b>	<b>73</b>
<b>3.2 DATA COLLECTION .....</b>	<b>74</b>
3.2.1 Website analysis.....	74
3.2.2 Literature survey .....	74
3.2.3 Statistical analysis .....	75
3.2.4 Customer reviews.....	75
<b>3.3 PROBLEM FORMULATIONS .....</b>	<b>75</b>

3.3.1 Modelling analytical hierarchy process .....	75
3.3.2 Modelling Page ranking .....	77
3.3.3 Decision table as fusion .....	77
<b>3.4 OBJECTIVE FUNCTIONS AND NOTATIONS .....</b>	<b>78</b>
<b>3.5 DEVELOPMENT OF THE PROPOSED PRAHP INTELLIGENT E-COMMERCE ASSURANCE MODEL .....</b>	<b>78</b>
3.5.1 Establishing a framework of intelligent e-commerce assurance .....	78
3.5.2 PRAHP mathematical and algorithmic analysis .....	84
<b>3.6 EVALUATION AND VALIDATION MECHANISM .....</b>	<b>89</b>
3.6.1 Trustworthy accuracy.....	89
3.6.2 Qualitative customer validation .....	90
3.6.3 Statistical hypothesis.....	91
<b>3.7 PRAHP DEPLOYMENT SCENARIO .....</b>	<b>92</b>
3.7.1 Trustworthy e-commerce website.....	92
3.7.2 Untrustworthy e-commerce website .....	93
<b>3.8 CHAPTER SUMMARY .....</b>	<b>94</b>
<b>CHAPTER 4 – EXPERIMENTAL EVALUATIONS AND RESULTS .....</b>	<b>95</b>
<b>4.1 OVERALL EXPERIMENTAL SETUP .....</b>	<b>95</b>
<b>4.2. EXPERIMENT 1: ANALYSIS OF E-COMMERCE ASSURANCE MODELS AND PRAHP ATTRIBUTES .....</b>	<b>96</b>
4.2.1. Introduction.....	96
4.2.2. Statistical survey on assurance model weaknesses .....	96
4.2.3 Statistical analysis on assurance attribute selection .....	97
<b>4.3 EXPERIMENT 2: INVESTIGATING CORRELATION OF PRAHP ASSURANCE ATTRIBUTES.....</b>	<b>103</b>
4.3.1 Introduction.....	103
4.3.2 Experimental setup.....	103
4.3.3 Descriptive and correlation analysis .....	106
<b>4.4 EXPERIMENT 3: PRAHP ASSURANCE FOR SIZEABLE GENERAL E-COMMERCE ENTERPRISES.....</b>	<b>109</b>
4.4.1. Introduction.....	109
4.4.2. Experimental setup: General e-commerce sites .....	109
4.4.3. PRAHP assurance for small and large general-commerce enterprises .....	110
4.4.4. Effects of varied damping factor $d$ on PRAHP .....	114
<b>4.5 EXPERIMENT 4: PRAHP EVALUATION ON PRIVATE AND PUBLIC CLOUD-BASED ASSURANCE.....</b>	<b>115</b>
4.5.1 Introduction.....	115



4.5.2 Experimental setup on cloud-based sites .....	115
4.5.3 Assurance of private and public e-commerce cloud sites .....	115
4.5.4 Effects of varied inbound links on PRAHP and second validation.....	122
<b>4.6 EXPERIMENT 5: PRAHP EVALUATION ON B2C AND B2B E-COMMERCE WEBSITES.....</b>	<b>123</b>
4.6.1 Experimental setup.....	123
4.6.2 Construction of AHP pairwise comparison matrix .....	124
4.6.3 Validation and accuracy of PRAHP results .....	129
4.6.4 How robust is the developed PRAHP? .....	130
<b>4.7 CHAPTER SUMMARY.....</b>	<b>131</b>
<b>CHAPTER 5: OPEN E-COMMERCE ASSURANCE RESEARCH.....</b>	<b>133</b>
5.1 INTRODUCTION.....	133
5.2 IMPLEMENTATION .....	133
5.3 PATTERN OF ARTICLES BY YEAR OF PUBLICATION.....	135
5.4 PATTERN OF ASSURANCE ARTICLES BY JOURNALS .....	135
5.5 PATTERN OF E-COMMERCE ASSURANCE ARTICLES BY TOPICS .....	136
5.6 OPEN RESEARCH QUESTIONS.....	139
5.7. COMPARATIVE EVALUATIONS OF E-COMMERCE ASSURANCE MODELS.....	139
5.7.1. Comparing PRAHP with classical approaches .....	141
5.7.2 An evaluation of PRAHP with other similar approaches.....	142
<b>CHAPTER 6: CONCLUSION AND FUTURE DIRECTIONS .....</b>	<b>144</b>
6.1 OVERVIEW OF THE STUDY/RESEARCH SUMMARY .....	144
6.2 RESOLUTIONS TO RESEARCH QUESTIONS.....	145
6.3 SUMMARY OF CONTRIBUTIONS.....	146
6.3.1 Theoretical contributions .....	146
6.3.2 Methodological contributions .....	148
6.3.3 Conclusions on the empirical study .....	149
6.4 RECOMMENDATIONS.....	151
6.5 LIMITATIONS AND FUTURE DIRECTIONS.....	152

# LIST OF FIGURES

<b>Figure 1:</b> UK's e-commerce revenue (adopted from [2]) .....	1
<b>Figure 2:</b> India's e-commerce revenue (adopted from [2]) .....	2
<b>Figure 3:</b> USA e-commerce revenue (adopted from [3]) .....	2
<b>Figure 4:</b> Cybercrime issues (adopted from [6]) .....	3
<b>Figure 5:</b> Research design steps.....	8
<b>Figure 6:</b> Investigative results on unaccredited websites .....	34
<b>Figure 7:</b> Investigative results on accredited websites .....	34
<b>Figure 8:</b> Survey of e-commerce attacks due to weaknesses of assurance models .....	35
<b>Figure 9:</b> Example of a web seal (adopted from [70]).....	49
<b>Figure 10:</b> Assurance methods (adopted from [60]) .....	51
<b>Figure 11:</b> Cloud computing types and deployment models (adopted from [12]).....	55
<b>Figure 12:</b> Page rank of a simple network (adopted from [86]) .....	65
<b>Figure 13 :</b> Example of an analytical hierachy process.....	67
<b>Figure 14:</b> Objective function (see online version for colours).....	78
<b>Figure 15:</b> Development of PRAHP model .....	79
<b>Figure 16:</b> Trustworthy website.....	92
<b>Figure 17:</b> Untrustworthy website.....	93
<b>Figure 18:</b> AHP weighting scale.....	95
<b>Figure 19:</b> Framework of PRAHP assurance model selection .....	98
<b>Figure 20:</b> Is legislation an assurance measure?.....	99
<b>Figure 21:</b> Are ISO standards an assurance measure?.....	100
<b>Figure 22:</b> Is policy an assurance measure?.....	101
<b>Figure 23:</b> Is advanced user security an assurance measure?.....	102
<b>Figure 24:</b> Is site availability an assurance measure? .....	103
<b>Figure 25:</b> Emerged correlational graph of the assurance measures .....	108
<b>Figure 26:</b> Varied damping factors.....	114
<b>Figure 27:</b> Varied inbound links for website I and F .....	122
<b>Figure 28:</b> Varied inbound links for website YZ And ST.....	131
<b>Figure 29:</b> Framework of open e-commerce assurance research .....	134
<b>Figure 30:</b> Distribution of articles by year .....	135
<b>Figure 31:</b> Pattern of assurance articles by journals .....	136
<b>Figure 32:</b> Pattern of assurance articles by topics.....	136
<b>Figure 33:</b> Number of B2C assurance articles.....	136
<b>Figure 34:</b> Number of B2B assurance articles .....	137
<b>Figure 35 :</b> Number of C2C assurance articles.....	137
<b>Figure 36:</b> Number of cloud-based articles .....	137
<b>Figure 37:</b> Number of M-commerce articles .....	138
<b>Figure 38:</b> Number of general e-commerce articles.....	138

# LIST OF TABLES

<b>Table 1:</b> Research synopsis .....	13
<b>Table 2:</b> Evaluations of e-commerce assurance model .....	36
<b>Table 3:</b> B2C assurance model comparisons.....	50
<b>Table 4:</b> B2B e-commerce assurance model comparisons .....	54
<b>Table 5:</b> Cloud assurance systems.....	60
<b>Table 6:</b> Comparison of cloud-based assurance models.....	64
<b>Table 7:</b> Decision table.....	71
<b>Table 8:</b> Sampled dataset from journal articles and real life data from e-commerce sites .....	107
<b>Table 9:</b> E-commerce website descriptions.....	109
<b>Table 10:</b> Pairwise comparison and AHP-1 with respect to the goal .....	110
<b>Table 11:</b> Last iteration for convergence and AHP-4 with respect to the goal .....	110
<b>Table 12:</b> Pairwise comparison and AHP-1 with respect to level 1 .....	111
<b>Table 13:</b> Last iteration for convergence .....	111
<b>Table 14:</b> Composite matrix percentage for website A .....	112
<b>Table 15:</b> Initial page rank matrix .....	112
<b>Table 16:</b> Final page rank matrix .....	113
<b>Table 17:</b> Validation results .....	114
<b>Table 18:</b> Cloud website descriptions .....	116
<b>Table 19:</b> Initial pairwise comparison and AHP-level 1 .....	116
<b>Table 20:</b> Final iteration for convergence and AHP- level 4.....	117
<b>Table 21:</b> Initial matrix and AHP-level 1 with respect to availability .....	118
<b>Table 22:</b> Final iteration for convergence and AHP level 4 with respect to availability.....	118
<b>Table 23:</b> Converged results with respect to all the variables .....	118
<b>Table 24:</b> Composite vector matrix percentage for all websites .....	119
<b>Table 25:</b> Initial page rank matrix .....	120
<b>Table 26:</b> Final page rank matrix converged at 17 <sup>th</sup> iteration.....	120
<b>Table 27:</b> Cloud websites ordered, ranked and rated according to importance.....	121
<b>Table 28:</b> Final PRAHP website ratings.....	121
<b>Table 29:</b> Website descriptions .....	123
<b>Table 30:</b> Initial pairwise comparison and AHP-level 1 .....	124
<b>Table 31:</b> Final iteration for convergence and AHP-level 4.....	125
<b>Table 32:</b> Initial matrix and AHP-level 1 with respect to policy .....	126
<b>Table 33:</b> Final iteration for convergence and AHP level with respect to policy .....	126
<b>Table 34:</b> Converged results with respect to all the variables for website GH .....	126
<b>Table 35:</b> Composite vector matrix from implementation of all websites .....	127
<b>Table 36:</b> Initial page rank matrix .....	128
<b>Table 37:</b> Final page rank matrix converged at the 21 <sup>st</sup> iteration .....	128
<b>Table 38:</b> B2B and B2C websites ordered, ranked and rated according to importance .....	129
<b>Table 39:</b> Final PRAHP website ratings.....	130
<b>Table 40:</b> Comparative evaluations of the proposed e-commerce assurance model and related e-commerce assurance models.....	140
<b>Table 41:</b> Comparative analysis of the PRAHP assurance model and other assurance methods .....	142
<b>Table 42:</b> Comparative analysis of PRAHP assurance features and other assurance methods .....	143

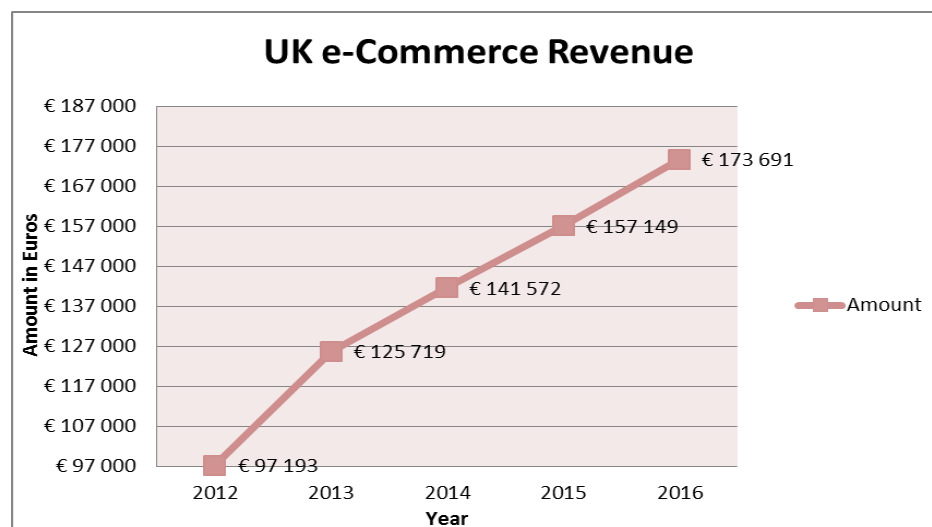
# LIST OF ABBREVIATIONS

<b>A</b>	Availability
<b>AL</b>	Adaptive Legislation
<b>AI</b>	Adaptive ISO Standards
<b>AS</b>	Advanced Security Login
<b>AHP</b>	Analytical Hierarchy Process
<b>B2B</b>	Business-to-Business
<b>B2C</b>	Business-to-Consumer
<b>BBB</b>	Better Business Bureau
<b>B2G</b>	Business-to-Government
<b>C2G</b>	Customer-to-Government
<b>G2G</b>	Government-to-Government
<b>G2C</b>	Government-to-Customer
<b>CR</b>	Consistency Ratio
<b>CSP</b>	Cloud Service Provider
<b>C2C</b>	Consumer- to-Consumer
<b>DT</b>	Decision Table
<b>E-Commerce</b>	Electronic Commerce
<b>EAR</b>	E-commerce Assurance Rating
<b>ECT ACT</b>	Electronic and Communications Act
<b>IPeA</b>	Internally Provided e-commerce Assurances
<b>HITS</b>	Hyperlink Induced Topic Search
<b>IoT</b>	Internet of Things
<b>ISO</b>	International Organisation for Standardisation
<b>P</b>	Policy
<b>PR</b>	Page Ranking
<b>PRAHP</b>	Page Ranking Analytical Hierarchy Process
<b>PCI DSS</b>	Payment Card Industry Data Security Standard
<b>POPI</b>	Protection of Personal Information Act

# CHAPTER 1: INTRODUCTION

## 1.1 BACKGROUND

E-commerce as a business enabler provides various benefits, such as convenience, efficiency and access to multiple resources in a short space of time to consumers conducting business in different countries. As a result, various countries, such as the United States of America (USA), India and the United Kingdom (UK), have shown a gradual increase in e-commerce sales, as illustrated in **Figures 1-3**. This demonstrates the contribution that e-commerce markets make to these countries' economy, hence its growing importance. Economically, e-commerce sales contribute to a country's gross domestic product [1]. **Figures 1, 2 and 3** show the revenue generated through e-commerce sales in the UK, India and USA respectively.



**Figure 1: UK's e-commerce revenue (adopted from [2])**

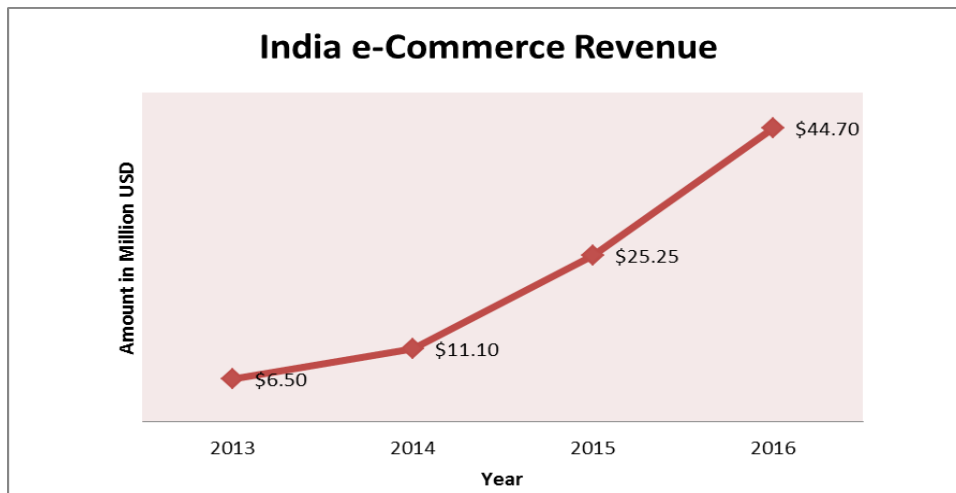


Figure 2: India's e-commerce revenue(adopted from [2])

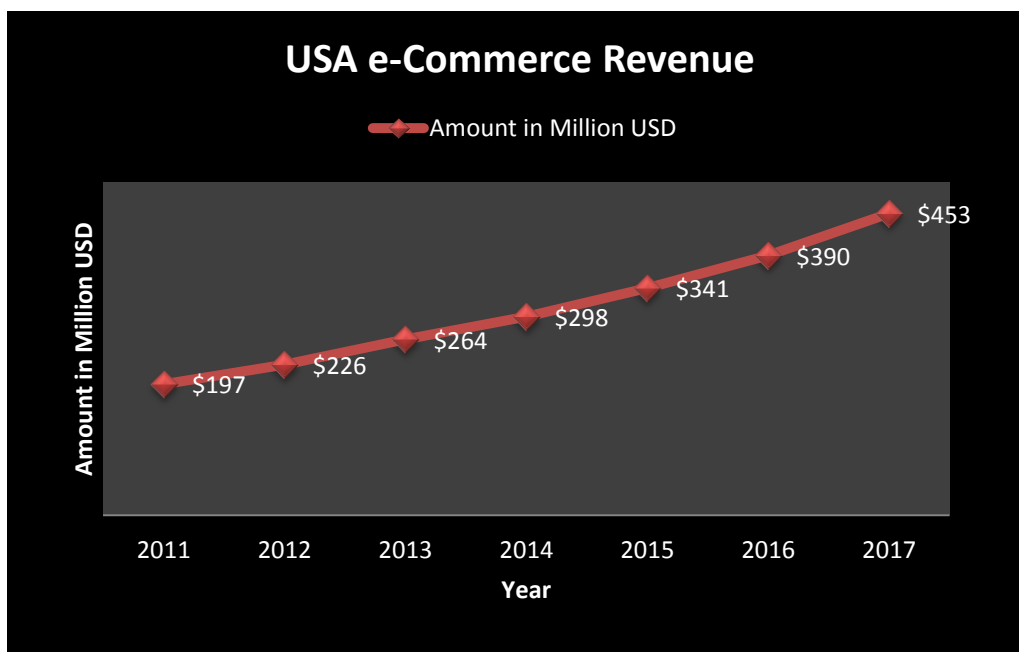
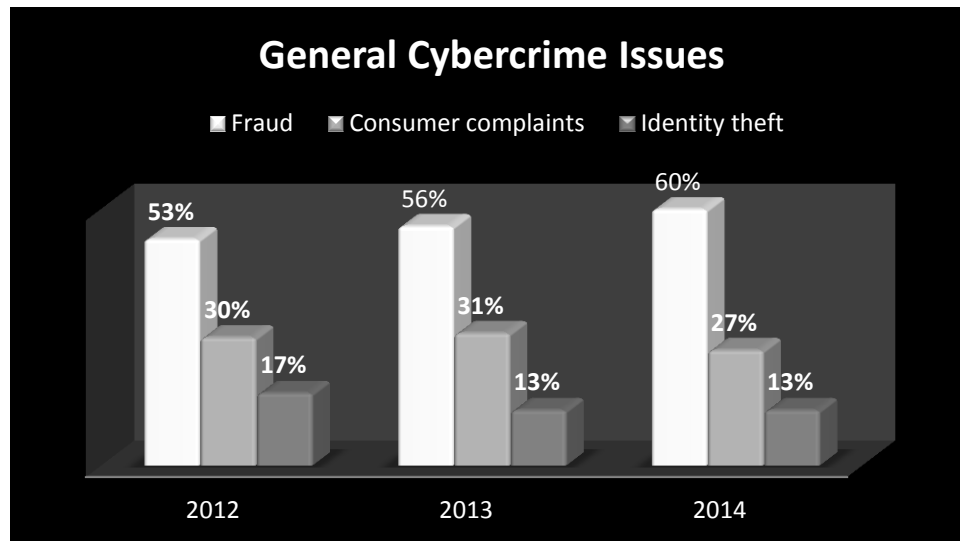


Figure 3: USA e-commerce revenue (Adopted from [3])

According to the sales figures displayed in **Figure 1**, it is evident that countries are gradually adopting e-commerce because of its benefits, such as being able to reduce unnecessary costs and reaching customers located in different countries through e-commerce platforms. Even though e-commerce has advantages, there are some negative aspects to it that need to be addressed. Because of the open nature of the internet, it is inherently susceptible to cyber-attacks, more especially cyber security attacks. Cases of identity theft have been reported by e-commerce stores where customers' credentials were fraudulently used for transacting purposes [4]. Other transactional risks, such as not being able to assess the comfort of items such as shoes, inhibit the adoption of e-commerce. **Figure 4** depicts the trend in cybercrime

issues from 2012 to 2014 on three specific categories, namely fraud, general cyber complaints and identity theft. Although these statistics do not extend to 2017, it is evident that there has been a gradual increase in e-commerce-related complaints owing to crime in e-commerce, affecting consumers. This research aims to investigate the specific issues that inhibit adoption and to illustrate how assurance models can be used to promote e-commerce assurance for trustworthiness.



**Figure 4: Cybercrime issues (adopted from [6])**

One form of internet-related attacks affecting users is phishing. Phishing is the ability by fraudsters to solicit confidential information from customers through social engineering and other technical methods [5]. Phishing attacks can be in the form of emails sent out to users to deceive them into thinking that the e-mail originates from trustworthy sources. The second source of phishing attacks arise from websites that have been specifically designed to deceive customers into thinking that they are official e-commerce sites, such as a bank or a legitimate credit card company [6]. Consumers often fall victim to phishing scams in instances where a user chooses to access an e-commerce site through a link and is then directed to a fictitious e-commerce site. The attackers do this for financial gain. Various measures have been implemented to promote consumer trust, such as policy statements on websites, awareness messages on banking institutions, websites and web seals that are displayed on the face of a website [7]. However, there are gaps that need be addressed, since these assurance measures do not provide comprehensive assurance to ensure trustworthiness, which guides a customer in making an informed purchasing decision.

Lack of trust in e-commerce is a major hindrance to e-commerce adoption [8]. In addition, lack of security and privacy in these environments is a threat to e-commerce adoption [8]. In order to promote e-commerce trust, various measures have been implemented to provide e-commerce assurance on the trustworthiness of e-commerce websites, but unfortunately they have some deficiencies that limit their effectiveness, such as inability to provide assurance on important attributes such as availability. As shown in **Figure 15**, an intelligent hybrid e-commerce assurance framework that integrates two powerful techniques has been proposed to address these gaps.

## 1.2 PROBLEM STATEMENT

The problem statement has been broken down into the following declarations.

*Existing e-commerce assurance models are good, but have gaps in promoting trustworthiness in online environments.*

“The publication of a privacy statement on the organization's website is already a standard practice and is used either as a trust building mechanism (Araujo, 2005) or as a legal safeguard (Fernback & Papacharissi, 2007). However, the presence of such a statement is not a guarantee that the organization will conform to it (Earp et al., 2005; Markel, 2005) or that the privacy statement corresponds to the tenets of fair information practice (Schwaig et al., 2006)” [9].

“Widely-used online ‘trust’ authorities issue certifications without substantial verification of recipients’ actual trustworthiness. This lax approach gives rise to adverse selection” [10].

Different e-commerce assurance models have been designed to help promote trustworthiness in online environments. However, many of these frameworks have shortcomings such as the inability to measure the level of compliance with legislation and other important attributes. The advent of cloud computing, more especially compliance with legislation, is fundamental considering cross-border transacting. Existing e-commerce assurance models such as the private cloud seal attest to the need for compliance with privacy legislation. However, it must be inclusive of other attributes that are necessary to provide adequate assurance in the cloud. The proposed model addresses these gaps through the inclusion of important assurance attributes to provide adequate assurance, which will bridge the gaps in existing assurance models.



**1.2.1** *Identifying assurance model attributes is key in determining the level of compliance and trustworthiness in cloud-based e-commerce.*

“Akin to cybercrime generally, cloud systems may be both the object and the subject of criminal activity. Rogue elements may target cloud systems with the intention of capturing or corrupting data.” [11].

“Despite the difficulty, for consumers, in understanding the differences between various assurance seals, their perception of security influences trust” [12].

The existing e-commerce assurance models are unclear in terms of the criteria that have been used to identify the attributes for assurance purposes. This creates a gap where assurance models might miss an opportunity to create trustworthiness in online environments.

**1.2.2** *Widespread occurrence of security incidents in cloud-based e-commerce affects consumer trust.*

“However, the storage of personal and sensitive information in the cloud raises concerns about the security and privacy of such information and how much the cloud can be trusted” [13].

“Cloud computing providers need to solve the common security challenges of traditional communication systems. At the same time they have to deal with other issues inherently introduced by the cloud computing paradigm itself”[14].

In ensuring the security of systems and information, the following principles must be maintained in cloud-based environments, i.e. confidentiality, integrity and availability of systems and information. Cloud consumers need assurance when it comes to security in the cloud in order to trust the e-commerce services of cloud service providers (CSPs). Unfortunately, holistic assurance on key attributes in the cloud is still lacking. The proposed model, the Page ranking analytical hierarchy process (PRAHP), provides holistic assurance on different important attributes such as availability and security to minimise the occurrence of security incidents.

**1.2.3** *Improving the level of security and trust on business-to-business and business-to-consumer e-commerce sites is a challenge.*

“With the growth of the Internet, B2C e-commerce has become a rapid area of expansion for many businesses. One barrier to success, however, has been a lack of consumer confidence in Web sites developed by companies. To help overcome this limitation, a number of separate providers have developed Web assurance services to provide these Web sites with institution-based trust”[15].

“Both ‘internally-provided’ (IPeA) and ‘externally-provided’ (EPeA) e-Assurances are being used by e-commerce businesses to build trust amongst consumers by alleviating concerns about the privacy and security of e-commerce transactions” [16].

Various deficiencies in business-to-business (B2B) and business-to-consumer (B2C) e-commerce assurance models exist, such as inability to provide comprehensive assurance that could ultimately result in a reduction in security incidents. PRAHP takes care of this shortcoming through a combination of assurances such as security, availability and International Organisation for Standardisation (ISO) standards and most importantly, customer inputs.

#### **1.2.4 *There is no or not enough work on a comprehensive roadmap of e-commerce assurance types.***

“Research should help us understand how trust is built and maintained in on-line exchange relationships, what role third-party assurance seals play in this process, and how they can be better applied to facilitate commercial exchanges in an electronic marketplace?” [17].

“Both practitioners and academic researchers in e-commerce have attempted diverse intervention strategies to promote online trust. One strategy adopts a third-party Web assurance seal to signal institution-based trustworthiness [35], particularly for small online retailers [58]. The academic literature, however, presents a pattern of inconsistent findings with regard to the effects of Web assurance seals on online consumer trust. For example, some previous studies find significant and positive impacts of Web assurance seals on consumer trust (e.g., [30, 42, 44, 53]), while others do not find a significant impact (e.g., [21, 24, 27, 35, 48, 58]). Thus, more research is warranted” [18].

Limited research has been conducted in the area of e-commerce assurance, which potentially makes it harder to come up with many recommendations for future research or a future roadmap for e-commerce research types that can be used by academics and practitioners. Failure to come up with a roadmap may worsen the impact of the issues that remain unaddressed.

### **1.3 RESEARCH OBJECTIVES**

The main objective of this study is:

**To develop an intelligent e-commerce assurance framework that will promote trustworthiness in online market environments.**

The need for such a framework is a result of the fact that in e-commerce there are various threats, such as security breaches, which potentially inhibit adoption. Considering that various e-commerce assurance models exist, shortcomings in these were identified. This study aims to develop an intelligent framework for promoting trustworthiness in online e-commerce environments.

This objective is supported by the following sub-objectives:

**1.3.1 To develop a reliable method of identifying e-commerce assurance model attributes as important compliance measures for e-commerce sites.** Various assurance attributes are used in the existing e-commerce assurance models, but some are more significant than others and clearly defined criteria are needed to guide attribute selection.

**1.3.2 To demonstrate the effectiveness of the intelligent framework in addressing security incidents in general e-commerce and on cloud-based platforms.** These demonstrations by the framework are necessary to reveal the robustness of the framework in different spheres of e-commerce when implemented.

**1.3.3 To determine if the control of weaknesses of the existing assurance models and third-party seals improves the level of security through the use of the framework, specifically in B2B and B2C e-commerce sites.** The weaknesses of the existing e-commerce assurance models and third party seals must be addressed in a way that will reflect an enhancement in the proposed framework.

**1.3.4 To design ways to generate a comprehensive roadmap for e-commerce assurance research types for future research by academics and practitioners.** This is done to facilitate the identification of other important e-commerce assurance issues, which are not covered by this research but still need further investigation.

## **1.4 RESEARCH QUESTIONS**

### **Main research question**

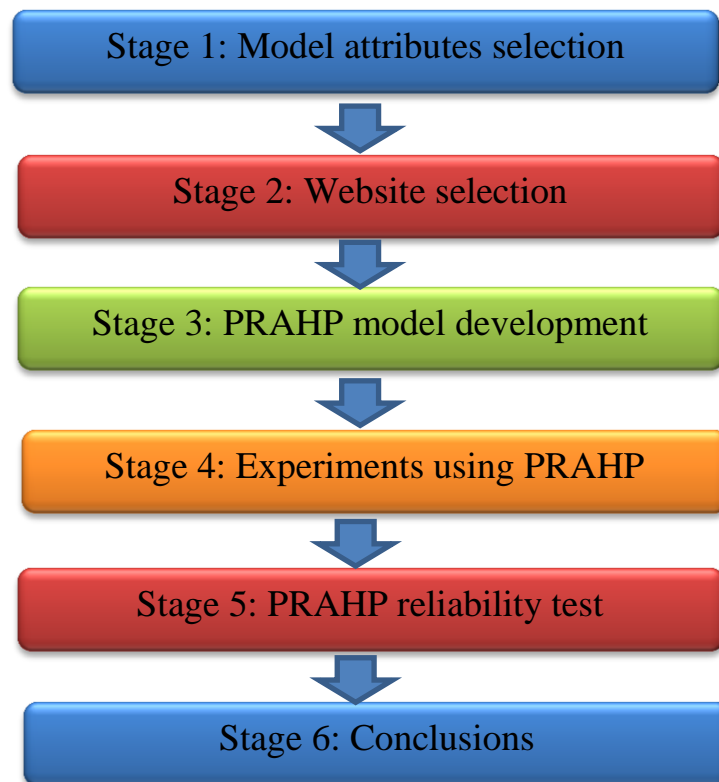
How can an intelligent framework of e-commerce assurance be developed to alleviate insecurity and promote trustworthiness in online market environments?

### Secondary research questions:

- How can the necessary assurance model attributes be identified to determine the level of compliance of e-commerce sites in the cyber world?
- To what extent can the framework address the widespread occurrence of insecurity incidents, such as credit card vulnerability, unavailability of cloud services and data insecurity, on cloud-based e-commerce?
- Does the level of information security on B2B and B2C e-commerce sites improve when using the framework after controlling weaknesses of assurance models and third-party security seals?
- How can a comprehensive roadmap for e-commerce assurance research types be investigated and structured to generate knowledge for both future academics and practitioners to safeguard online business and customers?

## 1.5 RESEARCH DESIGN

The research was designed in the manner that is illustrated in **Figure 5**.



**Figure 5: Research design steps**

The stages involved in this research are explained in the subsequent section:

### **Stage 1 - Model attributes selection**

Through the rigorous review of various assurance models from the literature, the important attributes worthy of inclusion in the model are identified. This phase is critical, because the attributes are the inputs to the model. After the selection of attributes, websites were selected to assess these attributes.

### **Stage 2 - Website selection**

A sample of websites selected for the study includes B2C, B2B, C2C and cloud-based e-commerce websites. In terms of size, websites varied from small to large, based on the number of inbound and outbound links.

### **Stage 3 - PRAHP model development**

This phase focuses on the development of the intelligent model called PRAHP, which is built on two computational techniques, i.e. the analytical hierarchy process (AHP) and Page ranking (PR). PR complements AHP through evidential reasoning.

### **Stage 4 - Experiments using PRAHP**

PRAHP is used to conduct numerous experiments on various e-commerce sites, i.e. B2C, B2B and cloud-based e-commerce websites. The experiments comprise three main stages, which are explained below:

1. **AHP assessment** - Websites are assessed through the PRAHP to determine the trustworthiness levels of the website.
2. **Customer feedback** -Third-party input in the form of customer comments on the trustworthiness of the website is obtained. This is then used to validate the assessment results of the AHP and PR techniques.
3. **Consensus results** - At this stage, the results from PRAHP are obtained regarding the trustworthiness of the websites.
4. **Reliability test**-The reliability of the PRAHP model is tested by varying the inbound and outbound links and observing the results.
5. **Conclusion** -The last phase is reaching a conclusion based on the results of the experiments on various e-commerce market types.

## **1.6 RESEARCH CONTRIBUTIONS**

### **1.6.1 Contributions to the scientific body of knowledge**

This research makes significant contributions to the e-commerce body of knowledge through the following:

- A newly proposed e-commerce assurance model, PRAHP, is developed, built on the AHP complemented with evidential reasoning from PR to provide assurance on security and trustworthiness issues on e-commerce.
- Trustworthiness is investigated, safety inspections are conducted and knowledge is generated as a reference guide to understand e-commerce trustworthiness in general and e-commerce assurance models in particular detail for B2B, B2C and cloud-based e-commerce environments.
- Experimental evaluations of the proposed assurance model are conducted on cloud-based e-commerce sites using real-life datasets. The results of these experiments revealed that PRAHP is a reliable measure of security assurance for the sustainability of cloud-based e-commerce. This was also supported through the outcome of varying inbound links, where it was apparent that as the number of inbound links increased, the rank of the website increased.
- PRAHP extracts real-life primary data directly from a selection of e-commerce websites where the results are validated by monitoring the effects of varied damping factor  $d$  on the model and checking the customer's comments.
- The e-commerce assurance learning structure represents the researcher's view of the e-commerce assurance literature that reveals e-commerce assurance topics. These have not received a lot of research attention leading to research questions to compile a roadmap on research issues for e-commerce assurance.

### **1.6.2 Declaration of publications resulting from this study**

The following publications relating to this research undertaking were produced, submitted and accepted by various accredited journals and conference proceedings:

## ACCREDITED JOURNALS

- **Mayayise, T.** and Osunmakinde, I.O. (2017) "Connective intelligence to stay safe while shopping online for e-products and e-services on business-2-business and business-2-consumer websites ", *International Journal of Business Information Systems (IJBIS)*, Inderscience Publishers, **ISSN online:**1746-0980, **Print:**1746-0972, (Accepted for publication, *Scopus(Elsevier)* indexed).
- **Mayayise, T.** and Osunmakinde, I. (2016), "Intelligent hybrid security model for a safer cloud-based e-commerce", *Kasmera Journal*, 44(1), pp. 322-342, ISSN 0075-5222, (*ISI journal*).
- **Mayayise, T.** and Osunmakinde, I.O. (2014) "E-commerce assurance models and trustworthiness issues: An empirical study", *International Journal Information Management and Computer Security*, Emerald Publishers, 22(1), pp. 76-96, ISSN: 0968-5227, (*Scopus indexed*).

## ACCREDITED CONFERENCES

- **Mayayise, T.** and Osunmakinde, I.O. (2015), Robustness of computational intelligent assurance models when assessing e-commerce sites, In *Proceedings of the Information Security for South Africa (ISSA 2015) Conference*, 14 – 16 August , South Africa, IEEE ISBN 978-1-4799-7755-0.
- **Mayayise, T.** and Osunmakinde, I.O., (2013), A compliant assurance model for assessing the trustworthiness of cloud-based e-commerce systems. In *Proceedings of the Information Security for South Africa (ISSA 2013) Conference*, 14 – 16 August, Johannesburg, South Africa, IEEE Catalog Number: CFP1366I-CDR, ISBN 978-1-4799-0809-7.
- Osunmakinde, I.O. and **Mayayise, T.** (2014). A learning structure of e-commerce assurance revealing hidden ICT topics in cyber world, *Proceedings of the 43rd Conference of the Southern African Computer Lecturers' Association (SACLA)* "ICT Education in the Cyber World", Port Elizabeth, South Africa, ISBN: 978 - 1 - 920508 – 34 – 0, pp 125 – 134. (DoE accredited.)

## 1.7 RESEARCH ETHICAL CONSIDERATIONS

As part of this study, ethical considerations were observed as required by the University of South Africa (UNISA).

Ethical clearance for this study has been obtained from the UNISA College of Science, Engineering and technology's (CSET) research and ethics committee under the following reference number: 112/TOM/2017/CSET\_SOC.

The researcher declares that this dissertation is her own work and that all sources used or quoted have been referenced and cited accordingly and no data or results were forged.

No part of this dissertation has been forged or plagiarised and Turnitin software was used to pick up any form of plagiarism. Mendeley referencing software was used for citations and referencing.

## **1.8 SCOPE AND CONTEXT OF THE STUDY**

### **1.8.1 Research scope**

Taking into account the diversity and latest developments in the e-commerce landscape, the scope of this research extends to the following e-commerce markets:

- B2B -This is where businesses transact with one another through the exchange of goods and services. An example of a B2B website is given in Oracle [19] and E-bay [20].
- B2C - In this type of e-commerce market, businesses exchange goods and services through e-commerce platforms with customers. An example of a B2C e-commerce market is given in Spree [21].
- At a high level the following e-commerce market types were also incorporated in certain parts of the study: mobile commerce and C2C e-commerce.
- Mobile commerce refers to the use of mobile device technologies such as cell phones for e-commerce purposes.
- C2C - In this e-commerce market, customers interact and transact with one other by purchasing of goods and services. An example of C2C is Gumtree [22].
- Small and large e-commerce sites – This is defined as local and international e-commerce markets. The size of a website is also determined by the number of inbound and outbound links.
- Cloud-based e-commerce environments – These entail e-commerce sites that use cloud information technology (IT).

A prototype of the PRAHP framework was developed as part of this study.

### **1.8.2 Research limitations**

This study was limited to only 10 e-commerce websites per experiment, resulting in 30 websites in total for this study, which excluded governmental institutions. As a result it cannot be determined what the results of the experiments would have been if the model had been tested in such environments. In terms of the attributes, only five important and impactful



attributes were identified and used; for instance, the researcher used one piece of legislation at a time for the assessment.

The scope of this study excludes e-commerce markets that deal directly with governmental e-commerce market types, such as business-to-government, customer-to-government, government-to-government (G2G) and government-to-customer (G2C).

## 1.9 RESEARCH SYNOPSIS

Table 1 provides an outline of the structure of the dissertation.

**Table 1: Research synopsis**

CHAPTER	TITLE	DESCRIPTION
<b>Chapter 2</b>	Literature survey and theoretical background	The literature that has been reviewed as part of this study, to explain important e-commerce types, challenges and risks and to explore various e-commerce assurance models, is reported. Arguments for and against different approaches to e-commerce assurance methods are presented in this chapter. An introduction and brief description of machine language theories used in this study are given here. Gaps in the existing literature are also highlighted in this chapter.
<b>Chapter 3</b>	Research design and methodology	This chapter explains the methodology strategy and design of this study in great detail.
<b>Chapter 4</b>	Experimental evaluations of PRAHP framework on e-commerce assurance	The experiments that were done on the B2C, B2B, private/public cloud environments and large and small e-commerce markets using the PRAHP assurance model are discussed in detail in this chapter. The ways in which these various e-commerce markets were evaluated and the criteria used are detailed.
<b>Chapter 5</b>	Open e-commerce assurance research	Patterns of open research items are presented in this chapter to highlight areas on which future research should focus. Recommended open research questions are also included in this section. A comparison of various e-commerce assurance models, including PRAHP, is done to show the strengths and weaknesses of every assurance model.
<b>Chapter 6</b>	Conclusion and future directions	This chapter concludes the study by highlighting the limitations of the study and explaining how the research questions were addressed in this study. Contributions of the study covering theoretical and methodological aspects are shared. Recommendations on future work are outlined.

## 1.10 CHAPTER SUMMARY

E-commerce has made tremendous contributions in countries where it has been adopted. However, there are risks that need to be addressed to ease the burden during adoption. Trust in e-commerce is an important determinant of adoption. This chapter introduced e-commerce in general, highlighting the advantages and disadvantages, backed up by some real-life statistics, as shown in **Figure 4** on cyber-crime and how this affects the issue of trust. The research objectives were also outlined in order to focus on the areas that will be covered, together with the objectives to be met.

This chapter discussed key challenges prevalent in e-commerce in formulating the research questions that the research objectives aim to meet. In terms of how the research questions would ultimately be answered, the scope of this paper was clearly defined. The limitations of this study were highlighted to provide further clarity on areas that have been excluded. The chapter outline for the remainder of the research was also covered in this chapter.

# **CHAPTER 2: LITERATURE SURVEY AND THEORETICAL BACKGROUND**

## **2.1 PRELIMINARIES**

This section discusses the literature relevant to the research topic that has been reviewed. Other sources of information, such as websites, were also examined in certain instances as additional references in the study. Various sources of information, such as journal publications, magazines, e-commerce websites and books, were consulted to identify the arguments for and against web assurance and related concepts and terms. The literature covered aspects of various types of e-commerce markets, risks and e-commerce assurance models and their challenges.

## **2.2 E-COMMERCE ASSURANCE MODELS AND TRUSTWORTHINESS ISSUES**

### **2.2.1 Trustworthiness fears**

The issue of trust has been identified in the field of e-commerce as an important aspect to consider when promoting e-commerce adoption. However, trust on its own does not have its own universally accepted definition, as each discipline simply defines trust in a manner that will suit the context of that area.

The internet of things (IoT) is an emerging area that will soon require the parties involved to operate from a position of trust. The IoT is defined as the connection of any device from a heterogeneous network environment that has an on and off switch to the internet or to each other [23]. The items covered under IoT include microwaves, smart phones, fridges, watches, lamps and headphones. People form part of these connections by being the users of these devices. The interconnectivity of various devices in IoT poses a challenge in terms of security breaches and reliability of information produced. Security and privacy of information have been identified as areas that need to be strengthened in the IoT environment for the management of trust [24].

As trust has been identified as an important factor to promote adoption for IoT, a trust management protocol has been proposed [25].

It looks at the social trust properties that need to be taken into account in these environments, such as honesty and cooperatives, which are somewhat similar to those that are important to be considered in the e-commerce environments.

Trust is characterised by a degree of uncertainty, dependence and vulnerability [23]. According to [26], trust is viewed in different ways, some of which are as follows:

Personality theorists view trust as an individual difference by considering the psychology of a person. The willingness to trust varies from person to person. Social psychologists view trust as an expectation of another party in any interaction. Trust as an expectation has to fulfil the following objectives (1): An expectation that the natural and social orders will be fulfilled; (2) An expectation that only technically competent individuals will ensure that the technical aspects in terms of performance will be met; and (3) An expectation that all parties who are obliged to carry out their duties will do so to the satisfaction of all parties concerned.

Trust is also viewed as an institutional matter by sociologists and psychologists. This refers to the view that trust should not be viewed as the responsibility of a single party, but as a contribution of collective units.

### **General methods of gaining trust**

From a social context, trust is gained from a number of areas. The following are the antecedents of trust in general [25]:

- **Trust based on personality** which refers to an individual's propensity to trust, which can be trust that comes from past experience or from a person's psychological state.
- **Cognitive based trust**, which is the trust that is obtained through having viewed or seen something without being disappointed.
- **Knowledge-based trust, which** is the trust that comes from knowing and being familiar with the parties at play.
- **Institution based trust**, which comes into place when a certain institution is given the power to approve or certify certain products or services, e.g. accreditation.

- **Calculative-based trust**, which entails beliefs that are rationally derived from costs and benefits.

In e-commerce, trust is of the utmost importance to the transacting parties because of the nature of the transacting environment, where almost everything is done in a virtualised manner. For instance, in the B2C e-commerce environment, when a customer buys goods or services in an unfamiliar e-commerce environment, there could be fears of fraud or of purchasing goods of inferior quality. Customers cannot be certain either that the information they capture on the e-commerce site will be stored securely and will not be transferred to unauthorised parties for other purposes, such as marketing [27]. There are many aspects that contribute to trustworthiness fears, which are briefly discussed in the subsequent section.

The virtual nature of the cyber world makes it susceptible to attacks, since there is no physical interaction between the transacting parties. E-commerce adoption is hindered by factors such as various forms of cyber-attacks, including website defacements, fictitious sites or credit card scams, which aim to defraud customers [28]. Unlike in a brick and mortar environment where a customer can easily return the goods to the vendor when dissatisfied, in e-commerce it is often difficult to lodge complaints, since not all countries have official internet complaint centres.

Some customers are reluctant to make online purchases for fear of having their credit and personal information divulged to unauthorised parties. When an e-commerce website is poorly designed and there is poor authentication, it can easily be compromised and customers' personal information can be stolen [29].

In B2B e-marketplaces, the transacting parties are likely to fear the possibility of the supplier not being able to deliver goods on time. In B2B e-commerce marketplaces there is a high risk of fraud, especially where the transacting parties have not been verified [7]. In 2011, there was a fraud case involving 2300 fraudulent accounts that were created in a B2B e-marketplace [26]. This was due to failure to conduct verification checks. The loss of money is likely to be a consequence of such fraudulent activities.

In the C2C e-commerce environment, trustworthiness fears are similar to those in the B2C and B2B e-commerce environments, except that owing to the nature of the platforms, a party to that relationship has to accept a certain amount of risk. The nature of most of the C2C e-

commerce platform involves the sale of individual items or unwanted goods. For many of these sites, very little information is required to open an account to transact [30].

A cell phone number or e-mail address is often sufficient to create an account. Criminals often target gullible customers to lure them into paying for non-existent goods before delivery in C2C environments. Criminals on these platforms create false advertisements, such as apartment rentals, which are marked as “urgent” in a sought-after residential area where the deposit payment is required urgently to secure the place. It is only after customers have paid the deposit that they realise that they have been defrauded, because as they move to occupy the said apartment, they find it already occupied by people who know nothing about the rental advertisement. A C2C e-commerce website that used to be a target for criminals is discussed in Gumtree [22].

In the cloud-based e-commerce environment where different deployment models exist, various risks are involved. It was noted that trust is significant in a cloud-based environment when discussing techniques that can assist in establishing trust in online environments. In the cloud where customer information can easily be disclosed or leaked, there needs to be an assurance method for establishing trustworthiness in online environments[31].

The techniques mentioned in the following section were noted as significant in establishing trust between customers and unknown entities in the cloud. The ability to negotiate trust, entity reputation, trust propagation and recommendation are techniques that facilitate building trust in cloud-based e-commerce environments. The open and borderless nature of the internet makes it difficult at times to ensure a trustworthy cloud-based environment. These challenges have increased the need for a trustworthy transacting platform.

Trust is the central theme in almost all e-commerce markets where the exchange of goods or services between unknown parties is involved.

Trust involves a certain level of subjective probability by which one party will perform a certain action before that particular action can be monitored [31]. Some authors describe trust as something consisting of two components or trusting beliefs and intentions with regard to willingness to depend on the other party to fulfil an obligation [32]. Trustworthiness in a commercial context is defined as the ability and willingness of a vendor to deliver the expected products or services, which are up to standard.

Because of cyber security attacks, consumers have fears about trustworthiness in the e-commerce space. For instance, risks associated with the loss of privacy or lack of security of personal information have been seen as a barrier in the past [8]. Privacy breaches encompass unauthorised disclosure of personal information and appropriation. Consumers are likely to feel unsafe when considering online transacting, especially if there is no assurance regarding restitution in the event of fraud [30]. Such uncertainties could inhibit e-commerce adoption.

### **2.2.2 E-commerce assurance model paradigms**

This section discusses the various e-commerce assurance model paradigms, highlighting the advantages and disadvantages. The aim is to uncover shortcomings in order to address them through a more comprehensive e-commerce assurance model. This supports the preceding section's findings.

#### **(a) Policy assurance models**

Different websites seek to provide some form of assurance to online customers through different means. One common method to provide such assurance is through policy statements, such as privacy policy statements that attempt to explain the vendor's responsibility to ensure protection of online personal information. Policy statements are normally displayed at the bottom of a website's home page, hyperlinked to the policy detail. The advantage of a policy assurance model is that it is common to various websites and that many users are familiar with such a form of assurance. The disadvantage is that some of the policy statements are quite long and users often do not have time to read them. Another disadvantage is lack of information on where breaches of these policy assurances can be reported. Examples of policy assurance models can be found in Amazon [33] .

#### **(b) Static seal assurance models**

The evolution of web assurance models has given rise to unique attributes of the various seals. A web seal is a seal of approval that marks a site as trustworthy or safe after having satisfied a set of requirements by a specific accreditation authority. A static seal assurance is a seal that is displayed on a certified site. It requires a user to click on the seal to understand what the seal stands for, since on the surface, the seal stays static.

The benefit of static seals is that they provide assurance on the trustworthiness of the sites on a broader spectrum of assurance areas. The disadvantage is that certain consumers do not know what the seals represent and consequently they may not even click to verify if the seal is valid or not.

### **(c) Variable seal assurance models**

Accreditation authorities have been working on improving static assurance seals, hence the invention of the variable seal assurance models. A variable seal assurance model is one that provides regular online updates on information on the assurance status of a particular website. The advantage of these types of models is that they provide online real-time information that is shown on the face of the seal. The disadvantage is that they do not show compliance-based information. An example of an assurance model that provides variable assurance is the site lock secure seal and the COMODO hacker-proof seal in [34].

### **2.2.3 Cloud-based assurance models in e-commerce**

Cloud computing can be defined as a model where information and related applications are stored in hidden or unknown systems, which can be accessed through terminals. It is a service to which users have access via the terminal to access data and applications. Cloud computing is meant to relieve the burden of acquiring, installing and maintaining applications from organisations that would prefer to have such services managed by the service provider. An example of a service in e-commerce for which many vendors use the cloud service is the outsourcing of the shopping cart service to another service provider. Cloud computing takes care of the management of the information and communication technology (ICT) infrastructure and other related services and thus provides business organisations with the opportunity to focus on their core business.

Cloud-based assurance models are in the form of certifications or compliance status achieved by the CSP to numerous standards. Amazon is a CSP and provides its customers with an assurance model that lists the types of certification received by the service provider, such as the International Organisation for Standardisation (ISO) 27001 [35] and the Payment Card Industry Standard [36]. The declaration of certification by the Amazon web services team is aimed at encouraging trust among its clients or merchants to use its technology platform.

There are numerous cloud assurance-related challenges, which are discussed below.



### **(a) Storage of personal credentials as an assurance challenge**

The cloud is basically a service that is available to a user, but the user is often not informed of where the personal or company information will be stored and whether the information will be shared or not. This is quite common in public cloud environments. A web assurance model that reveals how personal information in a cloud is managed and what type of legislation is applied to manage personal information would address this challenge to some degree.

### **(b) Security of data as an assurance challenge**

Online vendors would also need to rely on the policies and standards offered by the CSP. In terms of security of information, an online vendor who chooses to use the cloud service would have to rely on the security mechanisms offered by the CSP.

Web assurance should be provided continuously under stated criteria, which should be transparent to the merchants and different clients. Another challenge in the cloud computing environment is assigning responsibility in the event of a security breach in the cloud. Data breaches in a cloud are more severe in view of the impact of the damage, since more than one organisation is likely to be affected by such a breach.

Web assurance in a cloud environment is an area that needs attention, as many online vendors are expected to use the cloud services for business purposes.

The seal programme is one of the programmes aiming to address the existing gap in the seal industry specifically on cloud computing [37]. Cloud data privacy certification is a programme that has been designed to reduce assurance risks within the cloud computing environment [38].

Website assurance remains an important area to explore in cloud environments, considering the risks involved in such environments. Amazon prides itself on its ability to provide a secure website environment for business purposes, but that does not mean that every website that is affiliated to it will be protected by a standard security seal programme. The proposed web assurance and compliance rating model will assist in ensuring that CSPs match up and provide websites that are safe to use and are compliant with the relevant legislation and standards.

## **2.2.4 E-commerce applications**

Online vendors can choose a platform for their online business from different types of e-commerce applications. The choice of the e-commerce application is often influenced by factors such as whether an online vendor would like to develop an e-commerce application from scratch, or would like the website to be hosted by a service provider or would like to have an easily downloadable website application. Each choice has a set of advantages and disadvantages.

The benefit of developing a site from scratch is that a vendor will end up with a website that meets its needs. However, the disadvantage is that it might require resources coupled with expertise to design that particular website. Many organisations opt for a hosted site because it relieves them of the burden of maintaining and managing the website constantly. The risks associated with a hosted website include lack of control to implement risk-mitigating measures, such as loading relevant software patches to prevent the site from attacks.

### **(a) Open-source e-commerce applications**

Open-source e-commerce applications are designed and developed on the software that is available to users to use, copy, study and change through the availability of its source code. The advantage of open-source applications is that they are constantly undergoing refinement by peers to make them the best applications possible.

The disadvantage is lack of professional support; only community-based support is commonly available. An example of an open-source application is the Agora shopping cart. E-commerce assurance on open sources is given through a third-party accreditation authority.

### **(b) Proprietary e-commerce applications**

Proprietary e-commerce applications have been developed and are exclusively owned by certain vendors. The vendor of proprietary applications controls the distribution of the applications by having the users pay for the right to install and use the e-commerce applications. The strength of proprietary applications is that they are more reliable, since there is professional support and more control concerning software version releases. There are also additional security features, which are included as part of the package, such as encryption.

The disadvantage is that any improvements on the application would require payment for the enhancements, which renders proprietary applications more expensive. An example of a proprietary e-commerce application is Volusion [39]. Online businesses can also be designed on proprietary e-commerce applications such as the Volusion e-commerce application [39]. This application includes security features for the protection of personal information. In terms of e-commerce assurance, the gap that needs to be addressed on the e-commerce application is ensuring that all the sites are subject to a web seal programme, which will encourage online consumer trust.

### **2.2.5 Third-party seal assurances**

#### *(i) Privacy seal*

Many e-commerce websites have sought measures to create a trustworthiness transacting platform in order to gain consumer trust. One common method to create assurance is displaying a third-party seal [40]. Various accreditation institutions offer accreditation in specific areas [41]. For instance, there are third-party seals for privacy, security, fair business practices and others. A privacy seal aims to provide assurance to the customer regarding the data practices adopted by the online vendor to collect, process, store and to a certain extent distribute customer information [42]. In a nutshell, this type of seal aims to give assurance to customers and potential customers that the online store can be trusted with any piece of confidential information provided on such platforms. Considering that data privacy breaches are a common occurrence in cyber space, as in the case of Acer where numerous customer records were leaked through its e-commerce site [43], seals aim to mitigate such risks. These types of incidents are nothing new and even though privacy seals may be displayed to show that efforts have been made to prevent them from happening, breaches still occur. An example of a privacy seal is that of TRuste [37], which is issued to their e-commerce customers on satisfaction that the following requirements have been met:

**Data management practices** - The accrediting authority reviews and examines the data practices of online vendors for the website that needs to be certified. This process aims to confirm the organisation's practices in terms of the collection, storing and dissemination of customer information. It is a combination of manual and technical reviews to verify how data management practices are enforced. This is the first step in the accreditation process. In

addition to this, data scanning is done to confirm activities other than the data-collecting activities.

**Auditing report** - The accreditation authority examines the practices implemented by the e-commerce vendor and compares them to its set of principles and practices as guided by the applicable legislation and other best practice standards. Any deviations from the third-party practices will be raised in the form of audit findings, with recommendations on the controls that must be put in place to resolve the problems.

**Privacy policy or statement validation** - The third-party accreditation authority reviews the new privacy policy statement to ensure that it reflects its actual data management practices accurately, as noted at the data management practices phase.

**Accredited third-party privacy seal** - Once the accrediting authority is satisfied that all the findings that were raised in the initial stages of accreditation have been addressed, it issues the vendor with a privacy seal in the form of an electronic badge that is displayed on the website of the e-commerce vendor; it is linked to the website of the accrediting authority for verification purposes. The verification process is aimed at circumventing the piracy of seals by fraudulent websites. The verification process entails clicking on the seal, which directs a customer to the accreditation body's website where the validity of the privacy seal is confirmed.

**Dispute resolution** - In the case of privacy breaches or general privacy-related concerns, the third-party accreditation authority maps out a process that ensures that such matters are dealt with in a controlled and structured manner and that the online vendors maintain a level of accountability.

**Monitoring** - Technical tools are used to monitor the privacy risk of a website. The scanning of the site is done periodically to ensure that the relevant risks are identified timeously. Based on the process involved in obtaining accreditation to have a privacy seal, it is evident that customers are properly assessed before a seal is issued. The challenge with privacy seals is that it is not clear how such accreditations are revoked in the event of non-compliance with the set best practice standards.

Privacy seals are evolving as the need to be compliant with specific privacy laws starts to emerge. An example of such seals is the seal that certifies clients based on compliance with European Union laws [44].

## *(ii) Security seals*

Security of transactions in e-commerce environments is important. Theft of credit card information is a reality that often deters consumers and even potential consumers from buying goods online. E-commerce assurances have extended to covering specifically information security. Information is a broad subject, which ranges from the security of data to the technical measures required to process information in a secure manner.

An example of a website that has a third-party seal displayed on it is Loot [45], which displays the security trust seal by Thawte. The display of the seal certifies that all communications via the website are encrypted and that the strongest authentication mechanisms are used on the website. The online vendor simply needs to purchase the Secure Socket Layer web server certificates and install the seal that signifies that it is a secure site through the green display, which appears on the website. By clicking on the seal, details such as the name of the accredited company, domain name, country, validity and expiry date are shown. There are no strict requirements for acquiring the seal, except for the purchasing of the required certificates.

Other security third-party seals focus on other aspects of security, which could be classified as security soft issues, such as checking for phishing attacks etc. The McAfee Secure [46] seal is an example of a secure seal aimed at providing assurance to customers on the security and trustworthiness of a website.

This web seal is issued upon satisfaction by the accreditation body that the site is clear of any malicious software, phishing attacks and other harmful activities that could cause harm to a vendor's computer and customer information. Essentially five security aspects are checked in order to provide security assurance and issue the seal, namely:

*Malicious software checks* - Unwanted and harmful software is checked on the website and the relevant servers. If the checks reveal good standing, then a statement is issued and displayed to confirm that the site is clear of malicious software and can be trusted.

The problem with such statements is that it is not mentioned on the seal when these checks are conducted.

The second assurance check concerns theft of information, or phishing checks. This is also a privacy check in the sense that it checks for the unauthorised collection of data for purposes other than transacting.

*The Secure Socket Layer* certificate is checked for validity and assurance is given in the form of a statement that assures consumers that their information is protected through encryption, hence it is secure. Identity theft coverage is also provided for a certain number of days to customers who transact via the site and fall victim to such scams.

This is a good assurance mechanism, which encourages new online shoppers to transact in e-commerce.

The challenge with providing cover for only identity theft is that consumers may question why only identity theft cover is given and not cover against credit card fraud or theft or disclosure of confidential information. Lastly, with this particular security seal, consumers are assured of regular website scans that are conducted to ensure that all vulnerabilities are addressed to prevent exploitation by hackers. This security seal has proven to address certain security aspects that are not addressed by others, such as the Thwarte seal.

The shortcomings of this particular seal are that the detail provided on the seal is not convincing enough; for instance, no detail is given about the validity of the seal. It is also not clear whether the checks to be conducted are done using some online tools and how often these are done. According to the ISO 27001/27002 security standard, information security is the preservation of confidentiality, integrity and availability of information. From the checks that are conducted on the site, it is not clear how unavailability assurance is given.

Lastly, some security seals provide assurance based on online real-time scanning of vulnerabilities, which is done on the website, such as the COMODO hacker-proof seal [47].

This type of seal forms part of having the vendor site scanned daily for security vulnerabilities.

It also includes scanning to check for compliance with the payment card industry (PCI) standard requirements [36], even though these are not explicitly stated.

The good control offered by these kinds of seals is that they give a customer some level of assurance regarding the security of a website.

The seals that have been reviewed reveal that different vendors are seeking ways of providing assurance to customers on e-commerce environments. Many of these seals have strengths and weaknesses. For instance, most well-known seals are paid for, which can compromise the credibility of web seal providers.

### *(iii) Business practices seal*

Some e-commerce stores over time feel the need to give assurance regarding their business practices. The Better Business Bureau (BBB) [48] is an institution that accredits online stores once they have fulfilled a set of requirements. Because of the fraud that happens in online environments where seals are forged, the BBB seal has some advanced features, which assist in preventing illegal copying of a web seal. The feature on the BBB seal allows for the verification of the seal, which confirms that the seal is legitimate and belongs to that specific website.

The feature that shows the date the seal was issued and the expiry date validates the authenticity of the seal. This seal is ring-fenced to accredit businesses based in the USA and Canada. The benefits of applying for accreditation to use this seal are based on the following principles:

**Trust** - With this principle the requirement is that the online vendor must create and maintain a positive track record in the e-commerce marketplace.

**Advertising** – Plans have to be in place for advertising and selling goods and services in online environments. This is to promote the vendor through marketing.

**Honesty** – It must be possible to show the products sold on the platform completely and accurately. This is to prevent scenarios where misrepresentation of goods occurs and customers are misled. This principle does not include the quality of products and services.

**Transparency** - Many online businesses do not reveal much regarding their physical location, which can create doubt in the mind of a customer about where complaints can be lodged in the event that the online channels are not successful. This principle aims to get online stores to reveal details about their physical office locations, who the owners of the business are and all relevant policies and procedures.

**Honouring commitments** - Customers are more willing to buy from an online store that sets to deliver the required products by a certain date and is willing to keep the promise.

**Responsiveness** - The nature of online business might cause delays in terms of goods, consequently customers may need to log queries to get directions. If there are no channels for logging complaints and responding to these timeously, customers may lose confidence in the online vendor's ability to provide goods and services. This principle seeks to compel online businesses to respond quickly to customer complaints in a professional and trustworthy manner.

**Privacy** - In an e-commerce website, users are often required to provide their personal details for transacting purposes. With this principle BBB seeks to ensure that the online vendor maintains safe data management practices, which will ensure that the privacy of customers' personal information is maintained.

**Integrity** - This principle ensures integrity in handling e-commerce transactions. The advantage of this type of seal is that it seeks to compel online business to apply ethics and professionalism in business dealings while protecting the interest of customers. Some of these seals, such as the BBB seal, which was used as an example for review purposes, seek to provide the most comprehensive assurance possible on privacy and other principles that are customer-centric, but are deficient in other areas such as legislative matters, which should be incorporated, as most businesses are expected to comply with legislation.

#### *(iv) Trust seals*

There are seals that provide assurance at a certain level. In the preceding section, different types of seals were reviewed and arguments for and against the different types of seals were highlighted. Before some seals can be awarded, an online vendor goes through a rigorous accreditation process. WebTrust [49] is an example of a seal that is issued after an online vendor has satisfied a list of stipulated requirements. The independent practitioner carries out an audit on the particular vendor's online business. This business is audited based on an independent set of international principles and criteria meant for electronic commerce, which are jointly managed by the Canadian Institute of Chartered Accountants and the American Certified Institute of Public Accountants. Once the results of the verification audit agree, the online business satisfies the requirements for the seal to be issued and displayed on the company's website.



The principles focus on providing assurance based on the technical and non-technical controls on an e-commerce website. The WebTrust seals are only issued after a rigorous process has been concluded. The audit is strict and it is also ensured that the certificate authorities follow the stringent process of accrediting online businesses. Undoubtedly the WebTrust seal appears ideal compared to the first assurance seals that have been discussed. Unfortunately the thorough process is not enough to make it the seal of choice for most online vendors.

An assessment of the WebTrust seal was conducted to review its merits and demerits [48]. The assessment entailed a case study to review the merits and demerits of the seal. This seal was marked as one of the most comprehensive seals to be issued only to an organisation compliant with the accrediting bodies' requirements. The competition in the market is intense regarding assurance seal providers. Based on the findings of the study, the cost of acquiring the WebTrust [49] seal, in comparison to obtaining other seals, proved to be much higher. Secondly, there were no obvious benefits for businesses that had the seal displayed on their websites. This made the WebTrust less popular in the market and it was abandoned by one of the companies that had adopted it.

#### (v) *Guarantees*

Guarantees are another mechanism by which online stores aim to alleviate fears about trustworthiness in e-commerce. Guarantees are also meant to encourage consumers to transact, knowing that should something go wrong with the products or should they be dissatisfied, they can easily return the goods and be refunded.

Guarantees boost customer confidence when considering buying online, as they offer a buffer that gives customers a little relief in case things go wrong along the way.

The downfall could be if these guarantees are not enforced and customers are simply misled into committing their financial resources.

### **(a) Self-assurance measures**

Self-assurance measures are created by online businesses to assure customers of the trustworthiness of the transacting environment. Some of the self-assurance measures are discussed in the next section.

#### *(i) Online customer account*

In an effort to provide a safe online environment and to create a safe transacting platform, many online shops have a process allowing for the registration of customer credentials in order to create an online shopping account. Websites such as Superbalist [50] have a designed login process, which requires signing up for a free account using the customer's e-mail address or social media login credentials. This account is then used to transact and information such as credit card details is used. To access this account, a user name and password are required to gain access.

In as much as having a secure user account alleviates the risk of fraudulent transactions, there are other threats that create trustworthiness fears, such as hackers, that could result in data security breaches. To make login credentials difficult to compromise, they must be designed using strong mechanisms such as encryption and strong password management controls.

#### *(ii) Overall website features*

The professional look of a website makes it appear more attractive and trustworthy than a website that has been poorly designed. When a site is poorly designed, even if it is legitimate, it can easily be mistaken for a fictitious website. The features of a website alone are not sufficient to provide assurance, as additional assurances enhance the quality of assurance provided.

#### *(iii) Policies*

Many e-commerce websites contain policy statements that seek to provide self-assurance on specific aspects, i.e. privacy, security or refunds.

Policies are usually displayed on the face of a website on the home page, with simply a policy name hyperlinked to another page, which contains more detail.

Various e-commerce policies, such as the privacy policy, are required by law in countries such as the UK and Australia and must be displayed on the websites [51]. An example of a website with a privacy policy statement is Shop Goodwill [52]. In the category of policies is the website's terms of reference, which outline the rules by which the users of the website must abide, thus minimising spam. These policies are designed to protect the interests of online stores. An example of a terms of use policy statement is given in Webstore [53].

Return and refund policies are aimed at outlining the important requirements for being refunded in the event of non-delivery or dissatisfaction with the merchandise or service received. These policies provide assurance to users in the event of the purchasing deal failing. In certain instances the refund policy outlines that no refund will be made at all, regardless of the circumstances. An example of a website with a refund policy is Spree [21].

The disadvantage of relying only on policies for customer assurances is that often these policies must be read and some are quite detailed. Customers may not have the time to read the detail contained in the policy. Policies easily become outdated and may consequently not provide the relevant assurances pertinent to the existing threats. Another challenge is that some of the online vendors do not comply with their own policies.

#### *(iv) Technology assurances*

Online businesses aim to use various technology-based assurances to offer a certain level of assurance. Some of the technology assurances are in the form of online scanning tools. These tools provide detailed information on the health of a website, such as on the Ticket gateway website [54]. As a customer clicks on the seal to verify its legitimacy, it gives details of the last date and the time when the vulnerability scan was conducted and a note to confirm whether the site has passed the vulnerability scan or not. Despite this, the challenge remains with knowing the type of vulnerabilities that the tool checked for. Secondly, it is unclear if the seal would still be displayed in the event of a vulnerability scan that was unsuccessful.

In terms of technology assurances, there are also technical standards assurances. One of the standards commonly used in the e-commerce environment is the PCI data security standards (DSS) [36].

According to the PCI Security Standards Council, an organisation must satisfy all the requirements of the PCI DSS to be compliant [31].

Based on the milestones of the PCI DSS security standard, the milestones listed below must be met in order for an organisation to be certified as PCI DSS-compliant.

The security standard requires that firewall configuration be done correctly to protect mainly the cardholder's information and to ensure proper maintenance thereof. This is to prevent unauthorised access to the system and confidential information. The standard requires the use of unique passwords. As systems are installed, there are certain accounts that come with default passwords. These passwords must be changed into unique passwords that will be difficult to guess and to crack by hackers.

Unsecure cardholder's data remain vulnerable to all forms of attacks. The standard requires cardholder's data protection by enabling the correct settings on the firewalls and routers. It is also a requirement to ensure that the cardholder's data is encrypted during transmission, using the most secure means of encryption.

Viruses are a common threat in the cyber world and e-commerce. The regular use of up-to-date antivirus programs is required for the safety of online transacting information.

The organisation is required to be proactive in identifying the latest security vulnerabilities in the landscape in order to take proactive measures to secure the systems and maintain them better. The "*need to know*" principle must be upheld regarding access to cardholder information in the business. Access to information must only be granted to those individuals who need it based on their job descriptions. The standard further requires the assignment of unique login credentials to every person in an organisation who requires access to the system with confidential customer/cardholders' information. Physical access to systems and cardholders' data must be restricted to only authorised people. All access to important and confidential sources of information must be auditable. The last requirement of the standard is to test security systems and processes regularly, which covers vulnerability scanning. This is to protect the systems from exploitation of these vulnerabilities by hackers. Web seal providers provide assurance on this part of the standard, which simply confirms that the website has passed the vulnerability scans. An example of a vendor who provides a PCI compliance seal is Data Secure [55].

This standard is aimed at protecting consumers' secure online payment data. This standard looks at the security of the technology to determine if it is adequate to provide assurance to customers. The challenge with this standard is that it only focuses on technological assurance, but does not incorporate input from other sources to enhance the level of assurance. As a result, technology assurances in isolation may be limited.

#### *(v)Website verification tools*

Web verification tools offer information aimed at informing the customer about the trustworthiness of a website. The challenge with many of these tools is that they are not easily accessible or known to many people. Another challenge with some of these websites is that they are unstable and unavailable most of the time. Some of these web verification tools, even though they are detached from the website, provide some useful information, such as the location of the website servers, the domain age and trustworthiness ranking of the site. An example of a website tool that provides these services as a technical assurance measure is Scam Advisor [56]. The criterion that is used to rank a site as trustworthy is unknown. Other information, such as when the website was last refreshed, is open to many interpretations, considering the fact that some sites are rated trustworthy and popular, yet the website refresh date is old.

Website verification assurances are a useful way to assure customers of the trustworthiness of a website, particularly if the information provided is easy to understand and not open to many interpretations. Secondly, the assurances need to be in places customers will be able to access in order to obtain information before they can make important purchasing decisions.

#### **2.2.6 Investigation of weaknesses of third-party assurance methods**

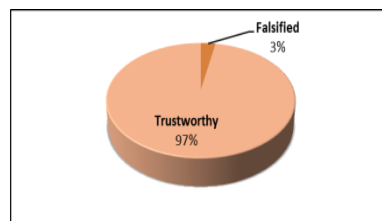
In e-commerce markets, there are challenges regarding the assurances provided to their customers. For instance, on some of the e-commerce sites, there are no policies providing assurance on the trustworthiness of the website. Since assurance is needed to boost trustworthiness on transacting platforms, it needs to be acknowledged that there are deficiencies in existing assurance methods, which might be worth addressing in future research.

As introduced in the preceding section, third-party seals are commonly used to provide assurance in e-commerce, from B2C to cloud-based e-commerce computing platforms.

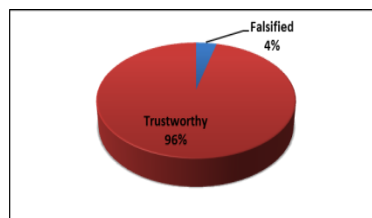
A study was conducted to examine a sample of websites accredited by different seal providers [11]. A comparison was made between accredited and unaccredited sites.

An assessment of policy compliance was conducted by using a tool on both the accredited and unaccredited websites.

The findings, as shown in **Figures 6 and 7**, revealed some surprising facts with regard to the accredited sites. The tool that was used to check for policy compliance revealed that 4% of the accredited sites did not comply with the requirements of the third-party accreditation body for policy. On uncertified sites, a lower percentage of 3% of the sites was found not to comply with the policy as per the tool. Some of the seals displayed on the certified, yet non-compliant, websites were Truste's [37] and the BBB seals [48]. These findings highlighted a few questions about the credibility of some of the seal providers. The fact that an online business must pay a fee to acquire the seal could possibly imply that generating revenue is a key driver in getting an online business accredited. These weaknesses of the existing assurance methods call for a more reliable and trustworthy assurance method, which will prioritise consumer concerns and provide unbiased guidance on the trustworthiness of a site.



**Figure 6: Investigative results on unaccredited websites**

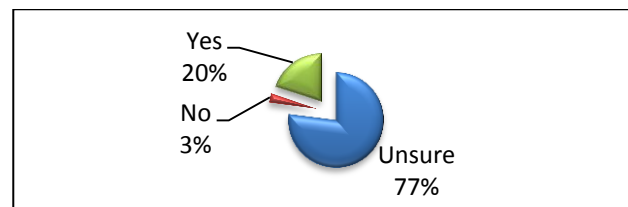


**Figure 7: Investigative results on accredited websites**

An empirical survey was conducted to look into the journal articles that referred to assurance models' related attacks. A sample of 30 journal articles from the Institute of Electrical and

Electronic Engineers (IEEE) and the Science Direct journals were reviewed. The articles covered the B2B and B2C e-commerce market literature.

With reference to the findings from the empirical survey, as shown in **Figure 8**, the following must be noted: Of the sampled journals, 77% could not explicitly link attacks on e-commerce to the challenges of assurance models, whereas 20% of the articles confirmed that some attacks happened because of weaknesses in the e-commerce assurance models. These results confirm that there are weaknesses in some of the e-commerce assurance models [57], which provide support for the direction of developing a more reliable and robust e-commerce assurance model for e-commerce markets.



**Figure 8: Survey on e-commerce attacks due to weaknesses of assurance models**

### **2.2.7 Important attributes of e-commerce assurance models**

Privacy and security of transactions in e-commerce are the major issues about which consumers tend to be greatly concerned when considering buying online. Assurance structures including attributes were assessed in a study and ranked by participants in order of importance [8]. The security of the website was identified as the most important attribute to consider in an e-commerce assurance. This was followed by privacy and return policies, which were also deemed important in an e-commerce environment to provide customer assurance. Shipping information and contact details were also regarded as important attributes. Customer testimonials, frequently asked questions and previous experience with the retailer were also identified as assurance attributes, although they were not ranked as important as the web seals.

Based on the view that e-commerce assurance models seek to provide assurance to consumers regarding the trustworthiness of a website, the factors affecting trust in the e-commerce environment were reviewed.

Based on the study, it was concluded that privacy, security concerns, the quality of the website information and overall reputation of the vendor determined trust [58]. This was a follow-up to a study conducted in 2002, which considered security, privacy and integrity as important attributes of assurance models.

The selection of attributes by web seal providers remains a controversial subject, as there appears to be no standard that guides the selection of attributes to be incorporated in a seal.

Most web seal providers consequently opt for simply identifying one attribute, e.g. privacy, and coming up with a privacy assurance model instead of combining a different set of attributes into one assurance model. This is another reason why many of the websites display more than one seal, which could cause some confusion, as some of the consumers may not be able to understand what the seal represents or the type of assurance provided.

## 2.2.8 Comparative evaluations of e-commerce assurance models

**Table 2** gives a comparison of the different assurance models reviewed in a summarised format. The comparison was done based on the combination of attributes.

**Table 2: Evaluations of e-commerce assurance model**

ASSURANCE METHOD	VISIBILITY	RELIABLE	INTER-ACTIVE	MULTI-ATTRIBUTE COMBINATION
Trust seal e.g. [49]	Yes	No	No	No
Business practices e.g. [58]	Yes	No	Limited	No
Technology assurance [34]	Yes	Yes	Yes	No
Policy [59]	No	No	Limited	No
Standards compliance scanning [36]	Yes	No	Limited	No
PRAHP	Yes	Yes	Yes	Yes



Based on the analysis of the assurance models, it is clear that most of the assurance models are visible enough when displayed on the website; a user would be able to see them.

The policies are often placed at the bottom of the website, written in very small font and hyperlinked. It would take a curious customer to search for the policy and read it.

Based on previous research, it is quite evident that seals cannot be regarded as reliable measures for granting assurance, as seals are issued for different reasons by accrediting institutions [11].

Most assurance methods allow for minimal interactivity by providing detailed information when one clicks on an icon regarding the validity of the seal. Other assurances models do not provide much interactivity, as a click lands one on the detail; it is left up to the reader to interpret and make sense of it.

A comprehensive assurance model consists of various attributes that give a better assurance level to a customer. The assurance is based on the collective assessment of all the attributes. Based on the information displayed in **Table 2**, it is evident that PRAHP consists of a number of attributes that make the model much more comprehensive compared to the rest of the assurance models.

### **2.2.9 Gaps identified in the literature**

Many researchers are starting to show interest in e-commerce assurance models. However, some areas still require much research, e.g. the use of assurance models in mobile e-commerce. This research has managed to bridge the gap in terms of coming up with an intelligent e-commerce assurance model (PRAHP), which can be used in the B2C, B2B and cloud-based e-commerce environments. Literature on some of the e-commerce markets proved to be limited and not much comparison could be drawn among the various e-commerce markets. However, this research has made a significant contribution to bridge those gaps in the literature through publications in accredited journals and conferences, as detailed in section 1.6.2.

The time lag between some of the researchers in the field of e-commerce assurance models was another limiting factor in that even though certain articles are recent, some of the research work was done more than 10 years ago.

Other than the assurance models used on websites in the form of seals, policies and security logins, the literature focused on theoretical trust frameworks without much practical application. The techniques related to some of the assurance models reviewed were not explained to give understanding of how they were designed to meet the requirements.

## **2.3 POPULAR AREAS OF E-COMMERCE ASSURANCE**

### **2.3.1 Business-to-consumer assurance**

The B2C e-commerce market type allows for the exchange of goods and services in electronic environments between businesses and consumers. Businesses create electronic platforms where they offer their services and products with the intention of selling these to consumers. An example of a B2C e-commerce market type is Loot [45]. Considering the nature of risks in e-commerce environments, trust is important, hence many e-commerce stores establish some kind of assurance in online stores to promote online customer trust. In the B2C environment, different types of assurance methods are used; a popular method is the refunds policy. This form of assurance is very important in this environment, as many customers need to know how complaints will be handled.

A B2C website that uses the refunds policy assurance method is Spree [21]. The advantage of having a well-written policy statement assurance method is that it is common to many users, as many online stores use it. The challenge with this assurance method is to ensure that the policy statement stays current and is revised to accommodate any process or external changes, such as new legislative requirements. Policies such as privacy policies are important to have, even for the online store itself, to protect it from potential lawsuits that may arise from data breaches.

### **2.3.2 Business-to-business assurance**

The B2B e-commerce market consists of an electronic platform that facilitates the exchange of goods and services between business organisations. Trust is fundamental in this e-commerce market in a similar way to the B2C e-commerce market. Various risks are associated with this e-commerce marketplace, for instance the risk of dealing with fictitious suppliers. The kinds of risks unique to this e-commerce market require a slightly different assurance mechanism to cater for them.

Alibaba [60] is an example of a B2B e-commerce market with a number of business affiliates.

However, this platform once became a serious victim of fraud because some of the businesses on it sold poor quality products and counterfeit items, which affected its ability to generate revenue. In an attempt to create trustworthy transacting platforms, various measures were deployed to provide that level of assurance, such as awarding different supplier statuses and vetting the trustworthiness of service and delivery of goods and services by a particular supplier. This vetting process is done by making an application and payment of a fee subject to endorsement and verification by the various verification authorities.

The benefits of this third-party verification system are that companies have the opportunity to attract more business counterparts to buy their goods and services. The disadvantage is that since a fee must be paid to obtain the accreditation, it may end up being a transactional issue, as the credibility of the third-party accreditation companies may be questioned. Other forms of assurance are used in the B2B e-commerce environment, such as policies and web seals, which are also used in the B2C e-commerce environment.

### **2.3.3 Cloud-based assurance**

Cloud computing refers to the provision of infrastructure as a service, platform as a service (PaaS) and software as a service (SaaS) to consumers. The cloud computing environment aims to ease the burden of many organisations because it takes away the responsibility of managing the technical aspects of technology and leaves the organisation to focus on the key issues of its business. There are different cloud computing service providers, including Google, Apple and Microsoft. Although there are merits to the adoption of cloud computing, the issue of privacy breaches cannot be overlooked [61].

An example of an assurance method on the cloud is trusted cloud privacy certification [38]. Data privacy is a serious issue in the cloud considering the type of services that are offered in the cloud. Privacy certification is aimed at providing assurance to customers concerning the data management services offered by the CSP. Proof of certification is shown in the form of a seal, which is displayed on the face of the website, normally on the home page. However, in a lot of fraud that happens, counterfeit seals are made by fictitious e-commerce sites to deceive customers who are not well acquainted with the seals. In order to minimise the risk of such incidents occurring, the certification bodies allow customers to verify the validity and

authenticity of seals through a search functionality, which is offered on the face of the website.

#### **2.3.4 Consumer-to-consumer assurance**

In the C2C e-commerce market, a platform is created for consumers to transact. These platforms include advertisements for new or second-hand products. On the C2C e-commerce platform most transactions are on a one-to-one basis and the trust factor is important, as fraud is prevalent in such environments. The owners of these platforms try to a greater extent to build in some controls, such as the advertiser's email address and contact telephone number, but such details can easily be obtained and used for fraudulent activities by some of the fraudsters.

An example of a C2C platform is Gumtree [62]. The type of assurance that is provided is in the form of rules, which in many cases can easily be broken without recourse. These rules include age restrictions for posting advertisements and a restriction on the number of accounts that an advertiser may have: no advertiser may have more than one account. These rules are easily broken, since they are difficult to enforce. The penalty for not adhering to the rules is simply disablement of the advertisement, which may not prevent fraudsters from manipulating the system in order to get what they want.

There have been numerous cases on C2C platforms where people have been defrauded of things such as rental deposits. The other downfall with many of the C2C platforms is that they offer a free platform to their users, but in reality the personal details supplied in terms of email addresses and contact telephone numbers are kept and could be given to other parties for marketing purposes. Many of these C2C platforms do not have policy statements, except conditions of use, which normally exempt the providers of the platforms from any disputes that may arise from non-fulfilment of transacting obligations. Assurance methods in the C2C platforms need to be looked at in order to protect customer information and make the platform trustworthy for transacting purposes.

#### **2.3.5 Mobile e-commerce assurance**

Mobility has created an opportunity for users to carry lighter and more portable computing devices, which gives them the ability to transact as they normally would with conventional IT

systems such as desktops computers. Mobile commerce refers to the use of wireless hand-held devices such as iPads and smartphones for buying goods and services.

Many e-commerce stores have a conventional online presence, which can be accessed via the normal web browsers, whereas mobile commerce provides customers with a platform to transact online. The mobile applications have limited assurance mechanisms compared to the conventional e-commerce websites. For instance, Spree [21] displays the Thwarte security seal on the face of its website, which is accessible through a conventional personal computer, whereas on the mobile device the assurance method is in the form of policy statements such as privacy and refund policies. This gap in mobile commerce could be indicative of shortcomings that need to be addressed in order to cater for similar assurances as on conventional e-commerce platforms such as desktop computers. Since mobile devices are susceptible to theft and loss, strong assurance measures are required to provide trustworthiness to encourage online shopping.

## **2.4 BUSINESS-TO-CONSUMER ASSURANCE**

### **2.4.1 Business-to-consumer assurance background**

In B2C e-commerce market buyers and sellers meet to exchange goods and services. One of the advantages of the B2C platform is that customers have the latitude to choose from a diverse number of online stores for convenience. What needs to be acknowledged is that the internet, as the main platform for facilitating online transacting, has some shortcomings to it which if not addressed could hinder adoption. There are risks pertaining to lack of recourse if the vendor fails to deliver the promised goods and services. Secondly, there is a risk of security of transactions as customers transact online. In essence, trust is an important determinant of the success of e-commerce transacting [63]. Trust can be defined as the expectation that parties will honour their commitments, i.e. they will negotiate fairly and not take advantage of the other party even when an opportunity to do so arises [64]. Trust is marked by the following attributes: uncertainty, being vulnerable and some element of dependence. In order for online shopping to take place, there must be an element of trustworthiness in the B2C e-commerce market.

To provide assurance regarding the trustworthiness of a transacting environment, vendors continue to design different types of assurance mechanisms to attract customers to buy in

their online stores. Various assurance methods have been adopted with the aim of creating a trustworthy shopping environment, i.e. policy statements and web assurance seals.

Security logins have also been designed to create a secure interface for users to utilise for transacting purposes.

Researchers have looked at various issues that they felt were assurance-related. These are explained in the following sections:

Policy statements in the B2C e-commerce market space are a common assurance method and are used simply to communicate management's intention regarding security, privacy and refund issues of a website in order to give assurance to the customer.

An online store may opt to have more than one policy, depending on the type of business in which it operates. An example of a policy statement in a B2C e-commerce store is given in Woolworths [65].

The advantage of using policy statements is that since they are commonly used, most users are quite familiar with their location and how to access them. However, the disadvantage of some of these policy statements is that at times they are not revised or when they are revised, old customers are not made aware of the new terms.

Third-party seals or seals of accreditation are another assurance method that is used in B2C e-commerce for assurance. To enable e-commerce businesses to have a seal displayed on their websites, they need to fulfil the stipulated requirements as outlined by the third-party authorities for accreditation. As assurance is sought on different e-commerce areas, various seals exist for B2C e-commerce environments. For instance, the privacy seal provides assurance on the privacy practices by the e-commerce business, particularly that their privacy practices are acceptable and meet certain industry expectations or standards [27]. Trust seals are another form of assurance, which provides assurance on the trustworthiness of the business. Other seals give assurance on the business practices followed by that particular online business. An example of this type of assurance seal is the BBB [42].

Web seals are a great help to some users who have prior knowledge and understanding of how they work and how to interpret the information written on the seal. Previous research highlighted that some users rarely take notice of website seals and what they actually stand

for [32]. This on its own can render the display of web seals ineffective in creating consumer assurance.

Seals are in the form of badges, which are very easy to forge. Even if users understand what a privacy seal stands for, without knowledge of how to check for the validity of the seal they remain vulnerable to attacks.

Another setback with regard to seals is the authenticity of those seals and the integrity of the certifying authorities [10]. The fact that a fee has to be paid to acquire the seal implies that if a third-party accreditation body is too stringent and does not certify as many websites as possible, it might soon go out of business. Seals are specific and tend to provide assurance in one area instead of providing a holistic view on the trustworthiness of a website.

These gaps can only be addressed by having an assurance model that is all-encompassing and factors in feedback/reviews by customers regarding the trustworthiness issues of that particular website.

#### **2.4.2 Business-to-consumer e-commerce risks**

The B2C e-commerce market is faced with numerous risks, of which some are unique to the B2C e-commerce environment. The uniqueness of some of these risks arises from the fact that customers are more vulnerable to any attack that could happen in that space. This does not negate the fact that the online business faces risks pertaining to fraud, in terms of dealing with fraudulent customers who may use fictitious payment details or stolen details to transact online. There are more risks that affect the online businesses in e-commerce environments, such as website defacements and phishing attacks. These could result in financial losses and reputational damage. Customers can easily blame the e-commerce vendor for investing in weak security controls. Defacements could result in unavailability of services and lead to customer frustration.

**(a) Security** of information, particularly personal information when transacting in the B2C e-commerce environment, is pertinent. There is a risk of unauthorised access to customer data or even theft of such information due to poor controls in some of the B2C e-commerce environments. Hacking into an e-commerce system could also result in a lot of customer data being compromised, where personal information could end up in the hands of unauthorised

people. An e-commerce website with a reputation of regular information security breaches is least likely to be trusted by customers.

Only when a website experiences no incidents of such a nature can customers feel comfortable to divulge confidential information. Strong authentication is important in ensuring protection of customer account information.

**(b) Privacy issues** - A single incident of compromising the database of an e-commerce store gives access to multiple resources, which could result in the compromise of privacy of customers' personal information. Privacy concerns in e-commerce generally have an impact on trust between customers and online merchants [65]. Privacy concerns that may affect customers are the collection of personal information such as credit card details and payment information.

Other concerns are the sharing of information with unauthorised parties where details such as customers' email addresses are exchanged without permission. The use of privacy seals is recognised as another control mechanism to mitigate privacy concerns. However, there are no guarantees that merchants will indeed abide by their own privacy policies.

**(c) Other risks** - A study was conducted to reveal the causes of challenges on the internet and e-commerce and the consequences of these [66]. The challenges were split into two categories, i.e. technical and non-technical. Non-technical sources of issues in e-commerce are among others phishing, spam emails, malware and online theft, which includes identity theft. These issues are concerned with the exposure of personal details such as customer contact details where phishing and spam emails can be sent. Although the issues identified as risks on the internet were not necessarily branded as specific to the B2C e-commerce market or to any category of e-commerce, they are generally applicable, as they have an impact on customer data. Previous research highlighted the consequences of the causes of these issues underpinning e-commerce risks [80]. Although the study did not categorise the e-commerce markets that would be affected or indicate how the identified risks could be averted, it gave background on internet risks.

Other e-commerce risks that have been identified include the non-delivery of goods and credit/debit card identity theft [18], which are among the most frequent complaints.



To ensure that an assurance method is effective in promoting trust, it must address the concerns of the customers.

### **2.4.3 Business-to-consumer assurance model challenges**

Different types of policies are used to provide consumer assurance in the e-commerce space, such as privacy, security, refund and charge policies. Online stores use policies that provide assurance on things they regard as related to their type of business. For instance, privacy policies are used to guide management on the collection of data and its storage and distribution.

The advantage of displaying a privacy policy is that such policies are quite common in different e-commerce sites, because consumers are often interested in how their information will be used [66].

The disadvantage of displaying privacy policies is that as legislation changes, the policy can become outdated and therefore not provide assurance based on the latest events. Some privacy policy statements are long and the use of legal jargon is common practice; consumers may consequently have difficulty with interpretation. In addition, privacy policies do not translate into compliance with relevant legislation. The length of privacy policies could discourage consumers from perusing such policies.

**(a) Refund policies** are written to give assurance on the monetary aspect of the e-commerce transaction. This could affect the consumer, especially if the goods are not received or the quality of goods received is substandard. An example of a refund policy is given in Walmart [67].

**(b) Charge policies** - These policies give a breakdown of the separate charges that are involved when acquiring goods from an online store, for instance shipping costs [68]. The advantage of these policies is that they give transparency on the pricing structure so that consumers can see what they are about to enter into.

**(c) Internet seals** - Third-party seals are used to give assurance in different areas, such as security, privacy, business practices and many other areas that are pertinent to the consumer.

In the B2C transacting relationship, consumers are most vulnerable because in the event of any loss, they are likely to suffer.

#### **2.4.4 Comparisons of various B2C assurance models**

Various e-commerce assurance models have been developed and continue to be developed to address some of the existing assurance gaps. A web assurance model was developed with the aim of encouraging online consumer trust in the B2C e-commerce environment [16]. The model made use of path analysis with latent variables, based on assurance, provider attributes, trust beliefs and outcomes. The model sought to address the assurance challenges by trying to establish the fundamental aspects of web assurance that affect trust and ultimately influence trust formation. Another objective was to understand trust formation and how it influences customers' outcome adjustments. This study provided a good foundation in terms of understanding the various factors that ultimately affect the formation of trust in the e-commerce environment as supported by the authors' findings, which revealed that assurances and individual provider attributes in e-commerce are positively and closely associated with various measures of trust.

In the literature review the researchers criticised other assurance measures, such as privacy policies, because policies are unreliable, as consumers cannot always believe what is written in a policy statement. Instead of dismissing such assurance measures, the study could have added more value by incorporating broader assurance measures and combining them in order to come up with a more comprehensive conclusion regarding the reliability of their proposed model. Policies in e-commerce have been included in the proposed research model based on the fact that they are still commonly used in the space, notwithstanding their shortcomings. The proposed model uses a reliable measure to identify the important assurance attributes so that the model can be relied upon, as the information that it gives is relevant for consumer decision-making.

##### **(a) Trust-building model**

A trust model was designed for electronic banking to create a trustworthy transacting platform [69]. The building blocks of the proposed model included the customer's perception of security and privacy.

The assurance attributes were identified following the careful review of prior literature, which was detailed. Other attributes included benevolence and integrity. Even though the

proposed framework [84] gave the basis of trustworthiness in terms of trust antecedents, it left many questions unanswered. The model did not detail how each antecedent would be assessed to determine the trustworthiness of an online banking website. It was also unclear what tests had been conducted to confirm the selection and reliability of those trust antecedents.

The essence of a relationship between a consumer and the business in e-commerce is based on a trust relationship. Without trust, parties cannot exchange goods and services in a virtual environment owing to fear of consequences, should anything go wrong in that relationship. Consumers are often hesitant to start sharing personal information and to transact from a vendor's website because of trust concerns. A trust-building model was developed [71] with the acknowledgement of the significance of consumer trust in an e-commerce relationship. Trust is explained as a phenomenon made up of trusting beliefs, perceptions of importance, integrity and trusting intentions, which are justified as willingness to depend on other parties.

The assurance model consisted of the following attributes: structural assurances, perceived vendor reputation and website quality.

**(b) Structural assurances** are those that are dependent on the features found on a website, which can also relate to the safety of a transacting platform. In the e-commerce environment, there is no physical contact, as everything is processed electronically.

**(c) Vendor reputation** is the reputation of a vendor on online platform matters. The more positive the reviews are regarding the vendor, the more trusted the vendor will be, as opposed to when the vendor is unknown to the customers or is known for wrong conduct, such as fraudulent scams.

**(d) Quality** entails the professional and consistent look of a website, which is important in gaining consumer trust, compared to a site that has no professional look. A poorly designed site creates room for doubt from consumers' perspective, as it may affect their trusting beliefs.

The model had to cover the following aspects: trust-building levers being perceived as vendor reputation and site quality, trust in the vendor and institutional structural factors.

The model was tested using a website and the results revealed that vendor reputation and quality are the elements vendors should consider when seeking to build consumer trust. The

model's lack of focus on certain aspects of trust, such as privacy or assurances customers need, limits its ability to address assurance matters in B2C e-commerce adequately.

*(i) Customer reviews for e-commerce assurance*

The various challenges that are prevalent in the e-commerce space make users extremely cautious when considering online transacting. Challenges such as processing transactions on technical platforms make the personal information susceptible to technical failures and consequent theft of information.

Numerous assurance models aim to address some of the e-commerce trust issues to a certain extent. In trying to attract online shoppers, many online stores make use of customer reviews that are testimonials to the service or goods received. These testimonials are meant to originate from real customers who have made use of the particular e-commerce website to buy goods and services. Customer reviews are easily accessible, as they are generally on the homepage of an e-commerce website. The reviews are easy to access and quite difficult to replicate, as they are specific to the products and services offered on a particular website. Customer reviews are more effective in promoting e-commerce trust compared to assurance seals [69]. This is based on the fact that the more positive the reviews are, the more sales and customers will be attracted to the site.

The downfall of customer reviews is that reviews can easily be faked or manipulated. Moreover, fictitious users can be created to provide positive ratings on a particular vendor site. Customer reviews cannot solely be relied upon as an assurance measure, taking into account the fraudulent activities that can be performed on some of the online vendor's websites.

On the other hand, unbiased, non-manipulated e-commerce customer reviews provide an independent view of how the users find the site.

*(ii) Web seals*

Different types of seals are used by B2C e-commerce stores. Some of the seals are internally generated and some are externally issued, but they all have a common purpose, which is to provide assurance.



**Figure 9: Example of a web seal (Adopted from [70])**

**Static seals** - Static seals require a click on the face of the seal to reveal detailed information on the validity or expiry of a web seal. Users who are not well versed in such assurance measures could easily assume that the display of such a seal does not require further verification. As a result they could fall prey to fictitious websites. Static seals are generally not interactive, as a simple click does not provide further details. Because of fraud in e-commerce markets, static seals are susceptible to forgery, as a badge can easily be created on the face of a website. An example of a static seal is displayed in **Figure 9**.

**Interactive seals** - These types of seals provide all the necessary details and are able to give the user an opportunity to select and verify the validity of the seal. Their limitation is in their inability to incorporate various assurance attributes to provide comprehensive assurance.

There are conflicting views regarding the level of awareness and impact of third-party seals [74]. Some consumers are aware of what the seals stand for, as they see the display on the website, but others are not aware of the seal and the seal does not influence their purchasing decisions at all. **Table 3** shows a summarised comparison of some of the B2C e-commerce assurance models.

**Table 3: B2C assurance model comparisons**

	Static Seal (e.g. BBB online [71])	Interactive Seals (e.g. [34])	Refund Policy	Customer Reviews
Interactive	No	Yes	No	No
Detailed review	Limited	Yes	Yes	Yes
Attributes composition	Limited	Limited	Limited	None
Easily accessible	Yes	Yes	Yes	Yes
Easily replicable	Yes	No	Yes	Yes

Based on the analysis of the various assurance models depicted in **Table 3**, it is evident that most e-commerce assurance models are easily accessible and are normally displayed on the face of the website. In terms of replicability, which in this context refers to the ability to replicate the assurance method for manipulation with malicious intentions, most of the assurance can easily be copied or forged and displayed on a website with the aim of deceiving customers.

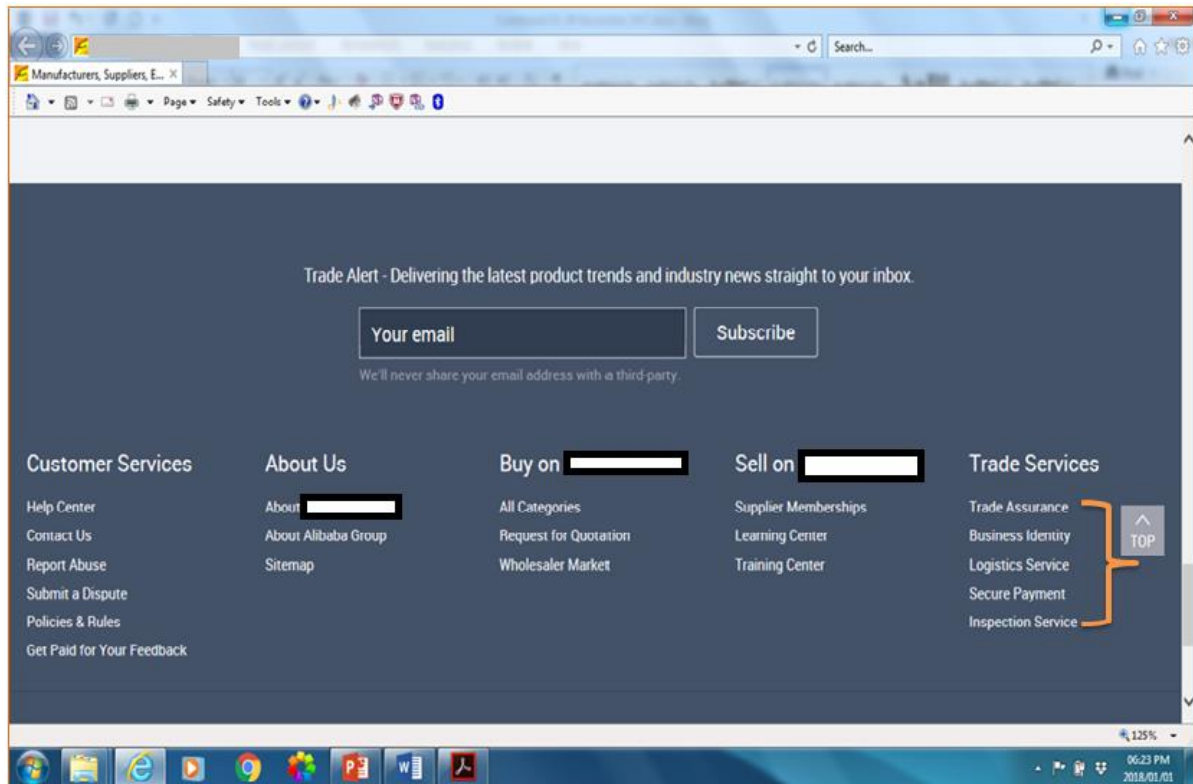
## **2.5 BUSINESS-TO-BUSINESS ASSURANCE**

### **2.5.1 Business-to-business assurance background**

The B2B e-commerce market is said to be a lot more profitable when compared with the B2C e-commerce market. This is generally due to the larger volume of trade, which is stated to be 10 times higher than in the B2C e-commerce market [72]. Considering the value of transactions in the B2B e-commerce market, there is a greater need for assurance by transacting parties on these platforms. Various assurance methods are used to provide assurance to the transacting parties, such as the ones shown in **Figure 10**.

B2B assurance methods seek to provide the specific assurances that are relevant in this e-commerce market type. These have gradually shifted from the use of hyperlinked policy statements to the use of trade assurances, which are pertinent in a setting where business partners are involved.

In comparison to B2C e-commerce assurances, B2B seems to offer more assurances, which may be linked to the value of transactions involved in this e-commerce platform setting.



**Figure 10: Assurance methods (adopted from [60])**

**Figure 10** depicts the assurance methods used by one of the largest B2B players. A set of assurances is offered to businesses to ensure a trustworthy transacting relationship. Trade assurances, business identity, secure and inspection services are some of the assurances that are offered to businesses to be included as part of their assurance methods. In addition, there are channels for logging complaints in the event of suspected fraud or abuse of the transacting relationships on these platforms.

Other assurance methods that are also offered in the B2C e-commerce environment, such as policies and seals, are also used in the B2B e-commerce platforms.

Trade assurance is another form of assurance offered in the B2B e-commerce environment. As the platform facilitates transacting between various suppliers, trade assurance seeks to provide assurance in terms of product quality protection, on-time shipment protection and 100% payment protection; in the event of loss/dissatisfaction, users are reimbursed [7]. This assurance method is similar to having insurance cover to take care of any loss that may arise as a result of customer dissatisfaction.

The crimes committed on B2B platforms have necessitated differentiation between fly-by-night businesses and authentic ones. This is done through supplier verification checks, which are done on the supplier; when all the requirements are met, a trust assurance seal of business identity is displayed next to the supplier's name.

Another form of assurance is the classification of suppliers into various categories. Various categories, such as gold supplier, and onsite checked status are used to highlight the fact that suppliers have met a certain level of success in terms of the application of good business practices [5]. In addition, suppliers have an opportunity to list other standards with which they comply when manufacturing their products, i.e. ISO 9001 quality standards.

Although these assurance measures are meant to provide trust to a greater extent, they do not cover every aspect of assurance. For instance, whether information that is exchanged during transacting will be shared with other parties or not is not always known.

### **2.5.2 Business-to-business e-commerce risks**

Various risks are prevalent in the B2B e-commerce environments and many of them are similar to B2C e-commerce risks. The next section discusses some of the B2B e-commerce risks from an assurance perspective.

In e-commerce, information is generally required to create a profile in an online environment for transacting purposes. In the event where login credentials of a business are required for transacting purposes, details of among others company names and physical or postal addresses are generally required. There is always a risk concerning where such information is stored, with whom it is going to be shared and for how long the information will be available on the system. Many e-commerce sites have created privacy policies that aim to address any discomfort that the transacting parties might experience with regard to the storage of that particular information.

**(a) Security and regulations** - Security of transactions in e-commerce is generally important, as trustworthiness is often linked to having a secure transacting platform.



E-commerce security is broken down into computer network security and e-commerce transacting security [78].

The computer network security dimension deals with the technical aspects of the environment, such as network and database system security. In this particular security dimension, a compromise on the technological side of the network could result in a breach in terms of confidentiality, integrity and availability of information or systems. The other dimension concerns the security of transactions, relating to the secure processing of transacting information. The risk in such a case is hacking and fraudulent transactions emanating from poor security controls. In the B2B e-commerce market security of transactions and network security are important to ensure trust among trading partners.

**(b) Loss of money** - In the B2B e-commerce markets where high-value transactions are processed, the issue of refunds is crucial. In the event of transacting with an unverified business partner, there is a risk of financial loss if refunds are not processed or not processed timeously.

Because of the way in which parties transact on this platform, there is always a risk of delays in obtaining the required merchandise once the order has been placed online.

If one party in the B2B relationship does not meet its obligations, it can be a challenge, as in many B2B exchange environments it is unclear who handles customer complaints or escalations. The B2B transacting platform is prone to the risk of fictitious suppliers who may defraud other businesses on the platform. These risks require strong assurance measures that will address most of the risks.

### **2.5.3 Business-to-business assurance model challenges**

The assurance challenges that are highlighted in section 2.4.3 for the B2C e-commerce markets are similar to the ones for B2B, more especially when it comes to the reviews, policy assurances and e-commerce seals challenges. An additional challenge with the B2B assurances is that sometimes assurances are used on the B2B platform itself and others are used directly by the suppliers. As a result it can be difficult to determine which assurance method to rely on.

### 2.5.4 Comparisons of various B2B assurance models

**Table 4: B2B e-commerce assurance model comparisons**

	Seals	Trade assurance	Policies	ISO Standards
Interactive	No	No	No	No
Detailed review	No	Yes	Yes	Yes
Comprehensive attributes composition	No	Yes	No	No
Easily accessible	Yes	Yes	Yes	No
Easily replicable	Yes	No	Yes	No

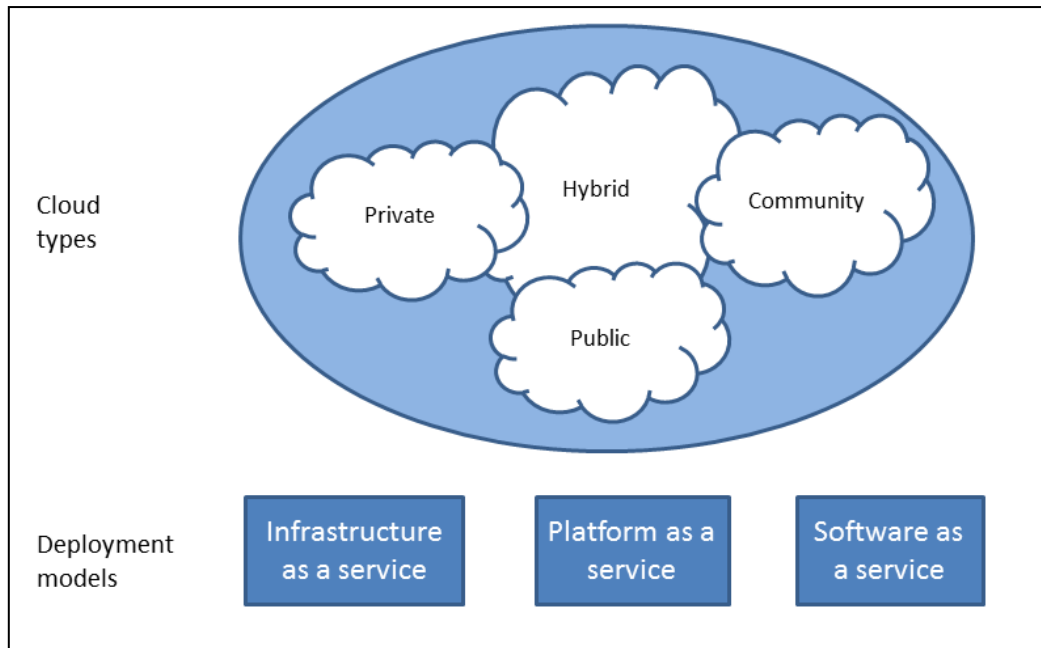
Table 4 shows a comparison of the various B2B e-commerce assurance models. Based on the analysis shown, it is evident that the trade assurance method is better than the rest, since it is a method that seeks to provide assurance on a number of attributes and it is easy to access the assurance service and the detailed review of what the assurance method stands for.

Other assurance methods, such as the ISO standards, e.g. ISO 27001, even though they are not easily replicable, tend to focus on specific areas of assurance, i.e. security of transactions in the environment.

## 2.6 CLOUD-BASED E-COMMERCE ASSURANCE

### 2.6.1 Cloud computing background

Cloud computing can be defined as the use of a network of remote servers that are hosted in different geographical locations from an organisation's local server to keep, process and manage the organisation's data.



**Figure 11: Cloud computing types and deployment models (adopted from [12])**

Cloud services have been classified into the following categories [12]:

*Software as a service* - In this category of cloud computing services, the provider licenses an application to the users either on subscription or as a free service. Some of the attributes of this service include having software managed in one central location and having many users use various devices that are able to access the software. The provider is then responsible for hosting the application, enhancements, bug fixes and any maintenance-related matters. An example of SaaS is Yahoo mail.

*Platform as a service* - This is the cloud service that provides the operating system capability to create, run and manage other applications in that environment without having to be concerned with providing the infrastructure to do so. The CSP provides the hardware and software to create such environments. These types of services are generally geared for software developers. An example of PaaS is Google App Engine.

*Infrastructure as a service*: This refers to the provision of services by the CSP, such as data storage and bandwidth among other cloud-computing services. These services extend to providing the capability to cloud service consumers to run their own software and applications through the cloud service infrastructure.

### 2.6.2 Cloud e-commerce risks

Cloud security has brought many benefits to various business organisations, but the unfortunate part is that the same advantages can also be disadvantages, depending on the view that is taken at a particular time. There are certain issues that are potential threats in cloud computing. These are discussed in the next section [14].

**Abuse of cloud access** - Malicious attackers of cloud services can take advantage of the anonymity of the CSPs and write malicious codes to attack users of the cloud computing services.

**Insecure interfaces** - Cloud services rely on the availability of certain key interfaces, e.g. application programming interface. In the event of the unavailability of certain secure applications, the application interfaces can be compromised.

**Malicious insiders** - The convergence of cloud service consumers and IT in cloud computing increases the risk of malicious insiders, which is exacerbated by lack of transparency of the provider processes and procedures.

**Shared technology issues** - As the resources are shared in the cloud computing space, because of scalability of resources, other components in the cloud that were not originally designed for that cloud computing space could cause security concerns.

**Data loss or leakage** - Because of the nature of the cloud environment in trying to accommodate various customers with similar needs in shared resources, one security breach could compromise a number of customers in the form of data loss or leakage.

**Account or service** -The exploitation of software vulnerabilities can result in an account or service hijacking, which can also affect many cloud service consumers.

#### (a) Privacy breaches

Cloud computing has brought tremendous benefits to business organisations by offering much needed services such as data storage and infrastructure provision. One of the cited benefits of the cloud is the provision of speed and ease, through which additional computer resources can be made available to meet business needs [73].

The type of cloud service offered exposes cloud service consumers to different risks, one of which is the breach of information privacy.

According to [61], information privacy is based on the view that information on people is theirs and they are ultimately responsible for controlling its dissemination. In the cloud, customers' personal details may be stored in a country server located in a different geographical location and the cloud service customer may not even be aware of all the parties that have access to such information.

#### **(b) Unauthorised access to customer and business data**

The risk of unauthorised access to customer data and other business data in a cloud environment is high. This is due to the fact that CSPs store this information, which can be accessed by means convenient to them and may not be the most secure. Secondly, the sharing of some resources by multiple customers could result in unauthorised access in the event of a data breach.

#### **(c) Security risks at the vendor**

Depending on the cloud service that has been chosen, the CSP is responsible for hosting that particular service. For instance, if infrastructure is taken to the cloud, then the infrastructure will be managed by the CSP as a service. Any security risks present at the vendor site, if exploited, could have a negative impact on cloud customers. Unlike in the traditional IT environment where every organisation had to implement security controls, cloud service consumers have to rely on other CSPs for the implementation of such controls. The issue of trust regarding hosting of cloud services is one of the inhibitors of cloud computing. A study was conducted to look at the requirements for critical infrastructure while considering moving into the cloud environment to preserve confidentiality and security of information [74] [73]. The requirements mentioned below were identified.

##### *(i) Online real-time support*

This is a requirement that emanates from a need to remain available even in the event of power interruptions and errors. This requires that CSPs be in a position to provide policies that explain how issues such as backups are handled.

### *(ii) Scalability*

The cloud resources must be able to handle variable amounts of loads of data at different times. This requires the CSP to demonstrate preparedness, ensuring that there will be no failure due to data load failures. The CSP is expected to demonstrate that data integrity will be maintained.

### *(iii) Security*

Logical and physical security aspects of a cloud are required for confidence in the safety and protection of data in the cloud. The CSP must be able to guarantee the security of data, considering the physical and logical access controls deployed in the cloud environment.

### *(iv) Availability assurances*

Many business organisations whose key business offering is not IT services may experience challenges in ensuring consistent systems uptime. As a result, many of these businesses choose cloud computing services because it relieves them of the responsibility for ensuring that systems are available at all times. In the selection process of a CSP, one of the important features of a good and reliable CSP is the ability to demonstrate that it can ensure availability of services and relevant resources.

For cloud consumers who are solely dependent on the service of a CSP for all their IT needs and who depend on cloud IT to conduct their business, the availability of cloud services is paramount. In the event where the CSP is brought down by hackers and the service becomes unavailable, it needs to be clear what the backup plans are.

### *(v) Cost-effectiveness*

The management of infrastructure and other technology services by an organisation can be a costly exercise, especially if these business organisations are not their key service interests. A CSP becomes attractive to potential customers if its service offering proves to be more cost-effective than self-management.

*(vi) Future capacity planning and provisioning*

To be chosen as a CSP, one of the requirements to be met is demonstrating that there is ongoing capacity planning and provision to cater for more demand to accommodate new requirements and customer needs. Failure to demonstrate this by showing how provisioning and capacity are catered for makes it difficult to attract customers.

*(vii) Legal assurances*

Cloud computing allows for cross-border transacting. This gets complicated when breaches occur and decisions have to be taken about the laws that will be applicable. CSPs should be able to give guidance on the laws with which they comply to make it clear what course of action will be taken in the event of a breach.

### **2.6.3 Cloud assurance method challenges**

There are limited assurance measures in the cloud, except for the different frameworks that have been designed to help prospective cloud customers select the appropriate CSP [79]. The frameworks outline important elements, such as the disaster recovery measures that must be taken into account when considering getting a CSP. Assurance measures that are aimed at incorporating technology, processes and people's interest still need to be considered and properly designed to promote trust.

#### **(a) Assurance systems for cloud-based e-commerce**

**Table 5** shows the different cloud-based e-commerce assurance systems found in a sample of websites.

**Table 5: Cloud assurance systems**

	Website Names				
Cloud Assurance Method	www.dimensiondata.com[74]	www.cloudnetwork.co.za[75]	www.hpe.com[76]	www.salesforce.com[77]	www.vmware.com[78]
Policies	√	×	√	√	√
Static Assurance Seal	×	×	x	x	x
Variable Assurance Seal	×	×	x	x	x
Availability	×	×	×	√	√
Legislative	√	×	√	√	x
Other Assurances	1.SLA 2.Terms of service	×	x	Security best practices – two-factor authentication	Terms of use

A review of CSPs' websites was conducted to determine the type of assurance methods that are deployed in their cloud environments. From the results of the analysis, it is evident that the commonly used assurance methods are policies, especially privacy policies, followed by availability monitoring of the cloud resources, which is followed by the legislative aspects that come into play in the cloud.

Despite the use of other assurance methods such as service level agreements (SLA), terms of service or use and strong security measures, the use of third-party accreditation in the form of seals is not catered for in the sample of websites reviewed.

## **(b) Attributes of intelligent cloud assurance models**

### *(i) Policies*

Cloud-based e-commerce environments are vulnerable to attacks, which are inherent in the traditional e-commerce environments. Some of these challenges include security and privacy issues, which come into play owing to cross-border transacting.



In 2011 when Sony's [79] network was hacked, it was linked to a hacker who rented out the service, as described in [33]. This incident and many others are a reminder of the risks that are prevalent in the cloud and need to be addressed, as they could inhibit adoption. As a result cloud service consumers require some form of assurance in order to feel safe. Just as in the traditional e-commerce environments, policy statements are being used as an assurance measure by CSPs. Policy statements are used to communicate the provider's intention to safeguard information, among other important issues that require some form of assurance. CSP policies should cover among others access control, privacy, backup and key management, as consumers need to know how such aspects are handled in the cloud to enable them to gain some level of trust. An example of a CSP with policy statements is given in [80]. Policies are a common way with which many customers are familiar as a source of assurance, but they have some shortcomings as sole assurance measures.

A common problem with some policy statements is that they are open-ended or one-sided, where the consumer does not feel assured at all because of their failure to articulate the measures that the service provider will take to protect customer information.

#### *(ii) Security standards*

The cloud-based e-commerce environment is complex and vulnerable to numerous risks related to lack of adequate controls to provide a reasonable level of assurance. Industry standards have been designed in an attempt to bring about alignment in terms of adherence to a minimum set of requirements.

In e-commerce, various standards have been developed to assist in securing online transactions such as the PCI DSS, which have been developed by the PCI DSS Council.

The SaaS model of the cloud must conform to the PCI DSS standard in order to provide assurance to consumers, especially regarding the safety of its data [81].

There are other standards that can be reused, even though they are not specifically cloud-based, for example the ISO 27001 security standard. Some CSPs do state compliance with the ISO security standards on their websites; however, the detail regarding the extent to which they are compliant is unverifiable. Secondly, it is up to a consumer to understand what that level of compliance entails, as cloud computing standards are required in order to achieve interoperability among different cloud environments to ensure stability, security and privacy on those platforms [14].

An example of a CSP that has cited compliance with standards is the Amazon web service, which cites compliance with the ISO 27001 security management standard, ISO 27017, ISO 27018 and the ISO 9001 standards. Although it is a commendable step to align to best practice standards in terms of cloud services, this information is scattered and left to the detail-orientated customer to peruse in order to determine the essence of compliance with the standards. In many instances the compliance is not stated by CSPs, whether in the form of an internal compliance assessment that was done or a rigorous process that was undertaken under the leadership of an independent certifying body. Without much information to qualify the display of the standards councils or authorities' logos on CSP's websites, very limited assurance can be created through the display of such badges [33].

### *(iii) Legislation/regulations*

Different laws and regulations are applicable in various countries and in specific sectors. For instance, there is safe harbour legislation with which the European Union and USA need to comply [82]. Laws are generally seen as an important assurance measure because the state uses coercive power to enforce compliance with its laws. This also allows consumers recourse against a CSP who fails to deliver satisfactory service [83]. This then provides a good level of assurance to the customer if a CSP is compliant with stated relevant laws. Because of the evolving nature of cloud computing, one of the challenges is for the CSPs who have not identified any laws to comply with in order to provide assurance.

### *(iv) Availability measures*

Some of the main reasons why many business organisations choose the cloud is cost saving and constant availability of business operations. Maintaining uptime is the responsibility of the CSP, since in many cases they are paid and expected to render that service. Availability in the cloud is defined as the percentage of time a customer is able to access a given cloud service [85]. Availability is one of the core building blocks of security, together with integrity and confidentiality. This is explained by the definition of information security given by the ISO 27001 security standard, which refers to information security as the preservation of confidentiality, integrity and availability.

A model of choosing an acceptable CSP called the technology acceptance model was developed [92]. This model incorporates availability as one of the trusting beliefs that must be considered when considering a CSP. This highlights yet again the importance of availability as an assurance attribute for a cloud assurance model. An example of a service provider that provides availability statistics for most of the cloud services and infrastructure that it provides is illustrated [87]. However, not every CSP has the tools to display the statistics. Furthermore, it must be noted that even if a CSP can show that its services have been available most of the time, one incident of unavailability could result in major reputational damage, especially if the unavailability is due to service compromise. In 2015 when there was an outage of Amazon [84] cloud services, many of its major clients were affected, as were its own services. The outage lasted for five hours, which meant that for online business, sales were affected negatively by this unavailability. The ability of a CSP to provide assurance on the availability of services is important in providing guidance to users on whether they should consider the use of such services or not.

#### *(v) Third-party accreditation*

Online risks and continuous cyber security threats have necessitated the development of assurance measures to encourage online trust among transacting parties.

Third-party accreditation is a common mechanism, which many cloud-based e-commerce platforms use in an attempt to create trust in their transacting parties. There is no guidance or standard indicating what accreditations should be based on and the criteria they should follow; it is all left to the third-party accreditors to scan the cloud computing threats and come up with a seal that will prevent discomfort for the various consumers. Examples of accreditation used in the cloud computing environment are Trusted Privacy and Trusted Cloud accreditation. Trusted Privacy accreditation simply states that the company has been endorsed to collect, store and dispose of personal information through good practices. Trusted Cloud services accreditation provides assurance that the certified organisation has fulfilled the requirements of the programme with regard to cloud computing.

The advantage of displaying evidence of accreditation on a website is that it gives assurance to users who are familiar with the seals. Web seals can easily be counterfeited, as they are easy to copy.

The trustworthiness of some of the websites that had seals displayed was questioned after an investigation revealed that websites with seals were no more trustworthy than those that displayed no seals [10].

#### 2.6.4 Comparisons of cloud assurance models

Table 6 gives a comparison of the various types of cloud-based assurance models based on comprehensiveness, adaptability, reliability and visibility.

**Table 6: Comparison of cloud-based assurance models**

	Comprehensive	Adaptable	Reliable	Visible
Monitoring tools	No	No	Yes	Yes
Policies	No	Yes	No	No
Seals	No	No	No	Yes
Regulation	No	Yes	Yes	No
Standards	No	Yes	Yes	No

Being comprehensive refers to the combination of more than one attribute to come up with the assurance model; based on the review; none of the cloud assurance models meets that criterion. Regulations and standards are much easier to rely on, since they had to pass through a thorough process.

## 2.7 SELECTED MACHINE LEARNING THEORIES

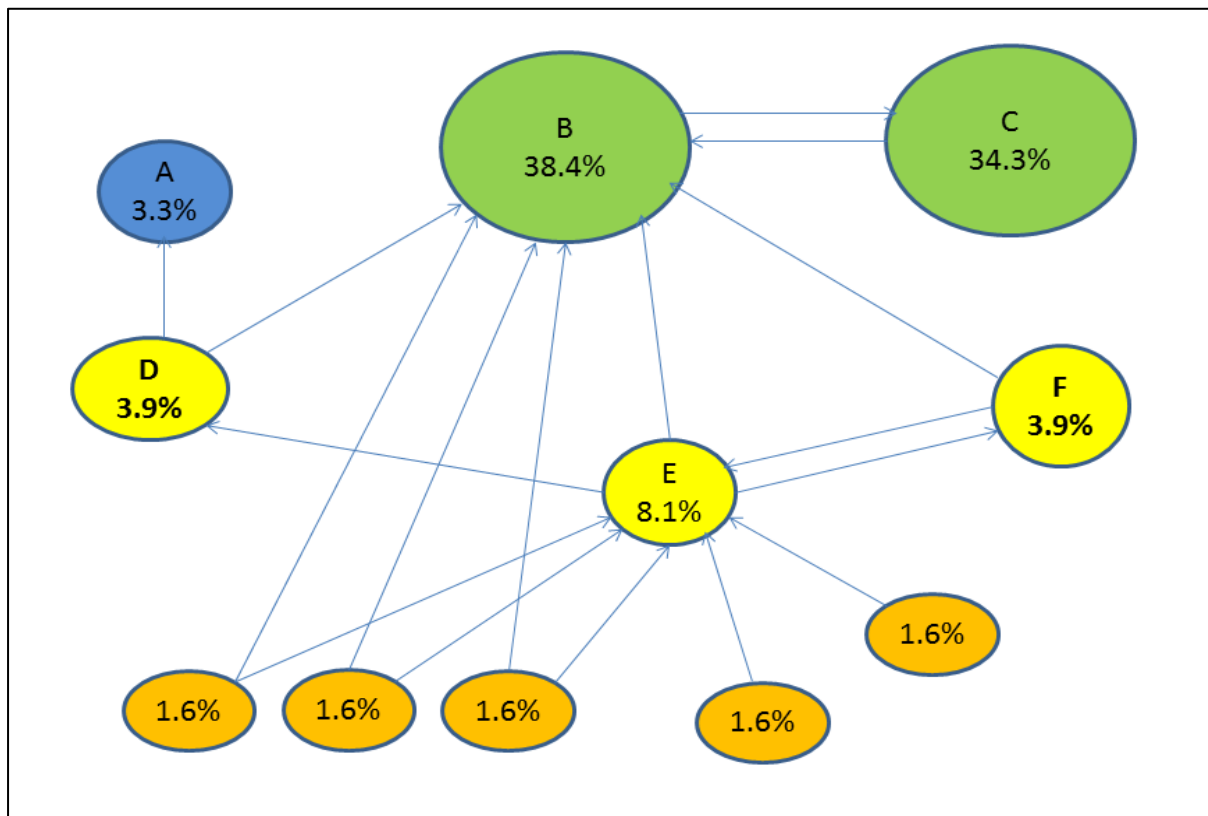
### 2.7.1 Page ranking

Different mechanisms and tools have been invented in an attempt to measure the importance of websites on the internet. Considering the increase in websites and information on the internet, the ranking of these websites in order of importance has become paramount. Websites can generally be ranked in order of importance by taking into account one of the following factors 1) the link structure of the website and 2) the type of content that is contained in that particular website. Page ranking is a technique that focuses on both criteria for the ranking of websites. It was developed by Larry Page [85]. In the case of ranking a website based on the content of a website or page, the following aspects are taken into account:

- The location of the specific terms on a web page
- The number of times the particular string appears on a page
- The number of terms that match with the string.

The link structure analysis works on the basis of the number of links connected to a particular web page. **Figure 12** shows the PR of a simple network of web pages.

Figure 12 demonstrates how the Page ranking algorithm works for a simple network. Website A links to all the websites through website D, as shown in the diagram, even though it has no outgoing links.



**Figure 12: Page rank for a simple network (adopted from [86])**

According to the information reflected in **Figure 12**, website E has lower PR than website C, despite the fact that website C has fewer links, as shown on the diagram, compared to website E. This is because website C has a strong link from website B, which is linked to many websites. Website A ultimately links to all other pages on the internet, although it has no outgoing links.

Various tools in the market use the PR algorithm. Some of these tools are Check Page Rank [87] and the PR checker tool [88].

PR uses a scale of 1 to 10, with 1 being the least important and 10 the most important website.

This technique is useful in providing a quantifiable measure of importance of a website so that it can give assurance on the significance of a website.

#### **2.7.1.1 Comparing Page ranking with hyperlink-induced topic search algorithm**

The increase in websites and increase in fraud have brought about a need for a method to identify popular and trustworthy websites. Various Page ranking methods have been developed in an attempt to close this gap. A hyperlink-induced topic search (HITS) algorithm is one of the methods that was developed by Jon Kleinberg [89] to try to address the problem of ranking websites. HITS operates through the calculation of the HUB and authority score of a particular node [90]. This algorithm is based on the premise that a web page serves two purposes: 1) A page that is pointed to by many hubs is called authority; (2) A hub is simply a page that contains links to authorities. The higher those authorities' score for that node are, the higher the number of incoming or outgoing edges.

HITS is applied in different areas, i.e. journal citations, social networks and various search engines.

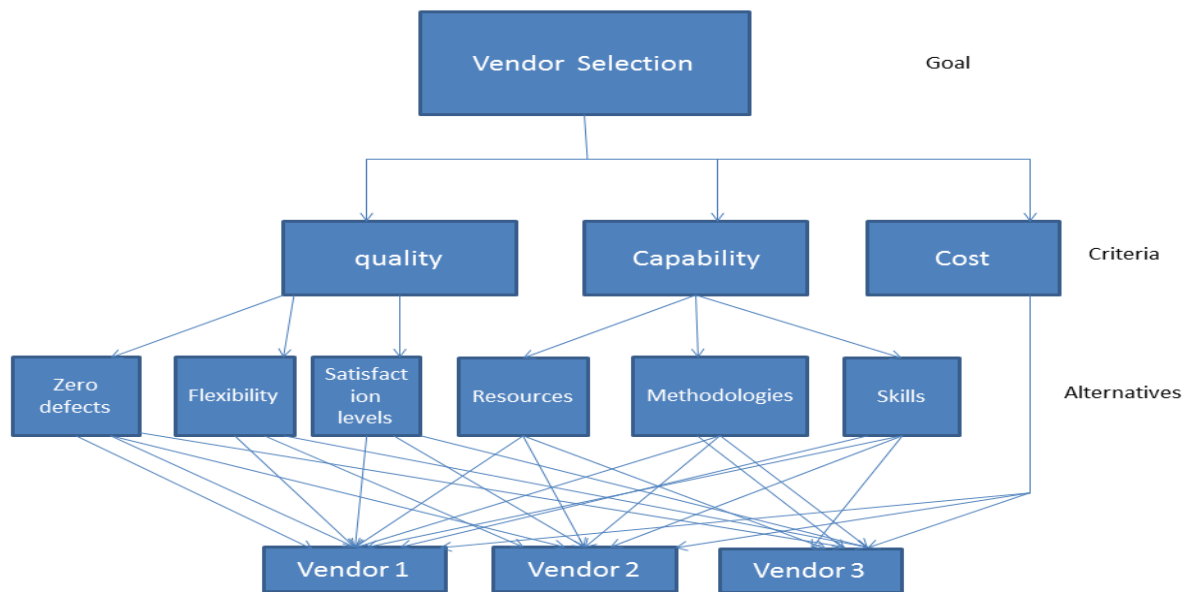
Based on the comparison of HITS and Page ranking as introduced in the preceding section, it is evident that Page ranking is a better web ranking method based on factors such as efficiency, feasibility and faster response time compared to the HITS website ranking method.

The researcher chose to use Page ranking based on the following advantages:

- In terms of the time it takes to respond to a query, Page ranking is much faster.
- It is less prone to spam as a result of localised links and it is more efficient, as it takes into account the quality of a page during indexing.
- Page ranking is considered a better modern-day option, as it performs calculations during indexing time instead of query time.

### 2.7.2 Analytical hierarchy process

**AHP** is a commonly used technique for decision-making, which is based on multiple criteria. The AHP is a structured technique of resolving complex problems [95]. This technique aims to resolve problems by first structuring them and then breaking them up into a hierarchical structure in order to analyse them. The AHP consists of three main hierarchical levels, i.e. the goal, criterion and alternatives, as illustrated in **Figure 13**.



**Figure 13: Example of an analytical hierarchy process**

The goal level looks at the overall aim that needs to be reached. For instance, the aim could be to select the most suitable vendor to render a service. The second stage looks at the criteria that will be used to achieve the goal; these include a group of factors to choose from in order to achieve the desired goal and in this case the criteria can be the quality of the vendor, capability and the cost of acquiring this vendor's services. On the third level, a number of alternatives could exist under the criteria, for instance for quality; the alternatives could be in terms of ensuring that the chosen vendor's products have zero defects and meet flexibility standards and that the vendor is able to achieve certain customer satisfaction levels. Thereafter vendor selection would be made considering these alternatives.

It is a technique that has been used and continues to be used in various industries and fields of study, including the fields of health, manufacturing and IT, among others. This technique has been used by decision makers and researchers in order to come to a final conclusion regarding different experiments [91]. AHP was used as a method to propose a model that would be used for selecting the industrial robot for grinding applications [92]. It is a method that is widely used because of its simplicity to resolve complex issues.

AHP works on the premise of the following methodological instructions: structuring complexity, measurement and combination.

A study to understand how AHP has been used in practice was conducted to determine how the criteria are defined and measured [93].

Six stages were identified for AHP based on this study [94].

**Problem definition** - This stage deals with identifying the problem that needs to be solved and clearly defining the problem. It is at this stage where all the assumptions are explicitly stated and the angle at which the final decision needs to be made is taken, so that at the end of the assessment, there is no ambiguity regarding resolution.

**Hierarchical structure of the decision-making** - AHP follows a hierarchical structure to problem resolution, which flows from the decision goal that needs to be reached, which filters down to the objectives at a broader perspective. These are then cascaded down onto the lower levels, which comprise the criteria and the alternatives. It is usually during this step that any alternatives that are regarded as irrelevant to the final decision are discarded by the decision makers.

**Matrices construction** - At this step, each element in the upper level of the hierarchy is compared to the corresponding one in the levels below it. This requires that a matrix be created for every criterion in the upper level. A scale of 1 to 9 is usually used to determine the number of times a particular element is dominant over the other from a criterion perspective. As the pairwise comparison is done using the matrices, when a value is assigned in every preferred criterion cell, the other cell is assigned the inverted value ( $1/\text{value}$ ). One of the strengths of AHP in decision-making is the precision and knowledge construction derived from comparison matrices. Every element of a problem is assigned a relative weight, which ultimately results in a hierarchy of relevance.



**Elements' relative weight calculation per level** - The following steps are involved in the calculation of the relative weight of the elements in a comparison matrix:

- (i) Add the value of the columns to normalise the matrix.
- (ii) Sum up the lines in the matrix to determine the relative priority of the criteria in a normalised matrix.
- (iii) Determine the consistency of the matrix through comparison of eigenvalues and the random consistency. The outcome is deemed satisfactory only when the consistency index is less than 0.1. In the event of inconsistencies in a matrix, the elements must be adjusted until consistency is reached. It is the decision maker's responsibility to review the comparison and make improvements where necessary.
- (iv) Conduct anterior steps for every criterion.
- (v) Compute the values of each alternative per criterion, based on the calculated priority.
- (vi) Sum up each alternative value to obtain the final value. The best alternative is chosen based on the highest priority.

**Review and balance the decision** - It is at this stage where the results obtained are brought into line with the expected decisions. A review of the previous steps is done to ensure that there are no flaws in the process, that the results can be trusted and that there are no gaps between what has been delivered and what was expected.

**Decision documentation** - All the necessary steps and facts that were considered throughout the process to reach a certain decision must be documented, which happens at this stage. This evidence is essential for future use, when this needs to be shared with third parties and for continuous improvement.

Based on a selection of articles published in various journals, AHP has been used for either selection or ranking purposes in various industries over the years [93]. In certain instances it was used on its own and in other instances it was used in combination with other techniques to complement one another and build reliability among the techniques.

### **2.7.2.1 Comparing AHP with other techniques**

#### **a) Bayesian decision theory**

Bayesian analysis is a statistical decision-making process that permits decision-making during uncertainty only with the help of additional information that seeks to reduce the impact of such information [93]. The Bayesian theorem is at the core of Bayesian analysis. It is a theorem that is based on the premise that causes are included in the final outcomes through conditional probabilities.

The attributes of the Bayesian theory are as follows [94]:

1. Reliance on a probabilistic model of an area
2. Openness to receive judgements that are subjective for empirical data
3. The Bayes Theorem is used as a primary mechanism for making adjustments when new information is considered.

The Bayesian theorem has often been used by researchers to supplement the AHP analysis for certain experiments. While the Bayes formula caters for the initial beliefs of decision makers in the implementation of certain events, it could always be reconsidered in the light of new or additional information or knowledge. It therefore means that the initial probabilities can be revised to determine the previous probabilities. Taking into account the fact that the decision-making process is complex and difficult to predict, the probabilities are often subjective, which weakens the validity of the Bayes formula.

#### **b) Dempster-Shafer theory of evidence**

The basis of this theory was established by the work done by Dempster, who established a system of upper and lower probabilities. Shafer, who was his student, extended the work on the theory by including more explanations on the belief functions, hence the theory was named after both of them[94]. The Dempster-Shafer theory is simply a theory for evidential reasoning.

It is a theory that focuses on probabilities with the upper and lower bounds. Researchers and various authors in the field of artificial intelligence have sought to popularise this technique

as a model for reasoning under uncertainty. It is regarded as a technique that offers more advantages when compared to traditional methods of statistics and the Bayesian decision theory. Even though the theory has some advantages over other methods, there has not been widespread use of this method [94]. The limited application of this theory makes it difficult to place reliance on it, since there are few cited examples of its application except in areas such as the following: Face recognition, medical diagnosis and other statistical classifications.

The AHP technique was chosen based on the following advantages:

- AHP offers a structure to problem-solving that makes it easy to adopt.
- It is a popular technique and has been applied in different fields of study.
- The fact that multi-criteria can be used extends its flexibility in ensuring that decisions are made after taking into account all the important attributes required for decision-making.
- AHP can be used to find solutions to complex problems, hence it is easy to apply in different industries and various research projects.

### 2.7.3 Decision table

A decision table is used to provide a simplified picture of presenting complex decision logic in a manner that is easy to understand. It consists of the following elements: actions, conditions and rules that need to be satisfied before a decision can be made. Conditions are all those aspects that must be considered before a decision can be taken. For instance, in a scenario where people need to withdraw money from an automated teller machine, they need to meet certain conditions, as shown in **Table 7**. They would need to have a valid bank card, pin code and sufficient funds in their account to withdraw the money. Only once those conditions have been met will the money be disbursed.

**Table 7: Decision table**

	Rule 1	Rule 2	Rule 3
<b>Conditions</b>			
Valid bank account card	T	T	F
Valid pin code	T	T	F
Withdrawal amount $\leq$ Balance	T	F	-
<b>Actions</b>			
Cash granted	T	F	F

Rules are a combination of conditions and actions that constitute the business decisions. The decision table will be incorporated as part of the proposed model for decision-making purposes.

## **2.8 CHAPTER SUMMARY**

The chapter started off with a detailed background on trustworthiness issues in e-commerce, highlighting the issues giving rise to trustworthiness fears in e-commerce environments. Contrasting views on e-commerce trustworthiness and e-commerce assurance matters by different researchers were discussed. In addition, various e-commerce assurance models were discussed, based on the following e-commerce assurance model classifications: B2C, B2B and cloud-based e-commerce assurance models. Strengths and weaknesses of the various e-commerce assurance models pertaining to the specific e-commerce types were identified. The highlighted gaps are the ones that need to be addressed by future e-commerce assurance models.

A learning structure of e-commerce assurance models was also mapped out, based on the reviewed literature covering various e-commerce market types, i.e. C2C, B2B and B2C. This learning structure is a roadmap that future researchers can use to investigate other related e-commerce assurance model issues.

The chapter was concluded by a discussion on selected machine learning, i.e. PR and AHP techniques, as these are important techniques for consideration in e-commerce assurance.

# CHAPTER 3: RESEARCH DESIGN AND METHODOLOGY

## 3.1 INTRODUCTION

Cybercrime makes the e-commerce space a risky environment for transacting purposes, which ultimately make consumers fearful and reluctant to buy goods and services online. The existing e-commerce assurance measures, such as web seals, have been applied to create trustworthiness assurance, but they have shortcomings that need to be addressed.

This chapter proposes an e-commerce assurance model, PRAHP, for trustworthiness in e-commerce environments. As explained in chapter 1, section 1.3, the objective of this research is to develop an intelligent e-commerce assurance framework, PRAHP, that will promote trustworthiness in e-commerce environments. The primary objective is supported by the following sub-objectives (from section 1.3):

1. To develop a reliable method of identifying e-commerce assurance model attributes as important compliance measures for e-commerce sites.
2. To demonstrate the effectiveness of the intelligent framework in addressing security incidents in general e-commerce and on cloud-based platforms.
3. To determine if the control of weaknesses of the existing assurance models and third-party seals improves the level of security through the use of the framework, specifically in the B2B and B2C e-commerce sites.
4. To design a way to generate a comprehensive roadmap for e-commerce assurance research types for future research by academics and practitioners.

The aim of this section is to discuss the method that was used to achieve the desired research objectives as illuminated through the research questions as well. For the purposes of this research, various methods were used to achieve specific research objectives. Triangulation [95], which is a combination of qualitative and quantitative methods, was used.

During website selection for experimental purposes, an analytical tool determining the size of a website was used. The selection of a sample of the websites was a qualitative process. Quantitative techniques that were adopted included PR and the AHP, although the analysis included some qualitative methods.

### **3.2 DATA COLLECTION**

This research study was conducted to cater for various e-commerce market types. In an effort to achieve the desired research objectives, specific data collection methods were used; these are discussed in sections 3.2.1-3.2.4.

#### **3.2.1 Website analysis**

Various e-commerce website types were reviewed manually and also through analytical tools [96]. The size of the website for some of the experiments was vital, considering the expected conclusion that had to be drawn for such experiments. The size of websites was determined based on the inbound, outbound and self-links.

Website analysis was an ideal form of collecting data, since the nature of the study was to collect real-life data, such as the number of website links and the type of service offering by the e-commerce store. The challenge with website analysis is that the information on production websites changes all the time, hence the results may differ over time, i.e. the number of website links. Website analysis was used in this study because of its reliability and accuracy as a data collection method.

#### **3.2.2 Literature survey**

The literature survey was conducted as part of this study in order to collect specific data to draw the correct conclusions. In order to identify the weaknesses of the existing e-commerce assurance models, a survey was conducted on a sample of the existing literature to determine the weaknesses of assurance models and ultimately to come up with a roadmap of e-commerce assurance issues. The survey was useful to come up with a reliable method of identifying e-commerce assurance model attributes. The literature used was mainly from accredited journals and thus provided a reliable basis. The shortcoming of collecting data through this method is that it can be very tedious, considering the number of journal articles that had to be reviewed. In instances where not much has been written about a specific e-

commerce subject, it can pose a challenge owing to insufficient support of the results and the conclusion.

### **3.2.3 Statistical analysis**

In order to demonstrate the effectiveness of the intelligent framework in addressing security incidents in general e-commerce and on cloud-based platforms, the AHP and PR techniques were used as mathematical tools. A decision table was used to aid in reaching a consensus decision. The use of statistical analysis tools provided efficient and accurate results. A possible challenge of statistical analysis is that some results are technical and they need more detailed explanations for the broader audience to understand.

### **3.2.4 Customer reviews**

Website customer reviews were used to collect data for input into the PRAHP model in order to support objectives 1, 2 and 3, as outlined in section 3.1. These reviews were used as validation mechanism for the website rating. In instances where PRAHP would show a website to be risky to transact from, a negative customer review would be an undisputed statement providing validation of the negative rating. Even though the reviews are reliable, it can be a challenge if, for instance, a website does not have the latest reviews.

## **3.3 PROBLEM FORMULATIONS**

This section details how the research problem was formulated mathematically using the AHP and PR techniques.

### **3.3.1 Modelling analytical hierarchy process**

The AHP technique as introduced in section 2.7.2 is one of the techniques employed to evaluate the assurance attributes used in this study. The assurance attributes that have been selected for the purposes of this study are: adaptive legislation (AL), adaptive ISO standards (AI), availability (A), advanced security login (AS) and policy (P).

The AHP technique is used to evaluate and obtain knowledge regarding every attribute in order to reach a decision based on multiple criteria. The technique achieves this objective by

providing structure to the assurance model attributes in the form of a hierarchy, where the lower level of the hierarchy is limited by the upper level.

The attributes are assessed ultimately to determine the website's state of trustworthiness in transacting platforms.

The steps involved in AHP are as follows:

1) Developing a judgement matrix

The AHP technique uses a rating scale of 1 to 9, which consists of the following variables: extremely unimportant, very strongly unimportant, strongly unimportant, moderately unimportant, of equal importance, moderately important, strongly more important, very strongly more important and extremely more important. This constitutes the judging matrix. The rating scale helps to determine the final website rating status for trustworthiness, i.e. red, amber and green (RAG). The judgement scenarios are developed through pairwise comparison.

$$Z = \{z_{ij}\} = \begin{bmatrix} z_{11} & \dots z_{1n} \\ \vdots & \vdots \\ z_{n1} & \dots z_{nn} \end{bmatrix} \quad (1)$$

where  $Z$  = comparison matrix. Equation 1 is used for the concurrent activation to complement the AHP and PR techniques.

- 2) In order to weigh the elements of the comparison matrix, the priority vector is used.
- 3) In order to determine the strength of the consistency ratio and to be able to check whether to evaluate the output or not, the eigenvalue is used.

$$CR = \frac{CI}{RI}, \quad CI = \frac{(X_{\max} - n)}{(n - 1)} \quad (2)$$

Where **RI** = Random index

- CR = Consistency ratio
- $n$  is the number of compared elements
- $X_{\max}$  is eigenvalue.



The eigenvalue is used to assess the strength of the consistency ratio (CR) of the comparative matrix to determine the need for output assessment. The outcome is deemed to have reached a satisfactory level only when  $CR < 10\%$  or  $CI < 0.1$ . In the event of inconsistencies in a matrix, the elements must be adjusted until consistency is reached.

### 3.3.2 Modelling Page ranking

PR is another component that forms part of the PRAHP model. It is a mathematical model, which is commonly used to rank websites based on the level of importance. As introduced in section 2.7.1, it is used to assess e-commerce assurance and provides an e-commerce assurance rating (EAR).

The EAR model is shown in equation (3).

$$EAR(A) = (1-d) + d\left(\frac{EAR(t1)}{c(t1)}\right) + ..... + d\left(\frac{EAR(tn)}{c(tn)}\right) \quad (3)$$

Based on the equation, for websites linking to A,  $c(t1) \dots (tn)$  are the number of outgoing links where  $d$  is a damping factor, which is normally set to 0.85. A low damping factor makes the calculations a lot easier and the convergence happens much more quickly.

Considering the fact that PR allocates a high rank to a node when it has many connections of other highly ranked nodes, it is useful in promoting website trustworthiness on e-commerce sites.

### 3.3.3 Decision table as fusion

The decision table is used on PRAHP to have clear rules to rank websites based on trustworthiness levels. The decision table works as explained in section 2.7.3 and it aims to assist in reaching a consensus decision through the fusion of two sets of complementary results, as illustrated in the upper section of **Figure 15**. This is further illustrated by the consensus results as shown in **Table 28** of the RAG status indications.

### 3.4 OBJECTIVE FUNCTIONS AND NOTATIONS

The main objective of this research was to develop a connective intelligent e-commerce assurance model, which uses complementary techniques to provide assurance for B2B and B2C e-commerce websites and cloud-based e-commerce environments. The objective of this research is summarised in **Figure 14**. The techniques involved in the assessment of the attributes are PR and the AHP. The results of the joint assessment by both techniques provide information on the trustworthiness of a website; for instance a website that is found to be untrustworthy is flagged “red” and one that is partially untrustworthy is flagged “amber”, as depicted in **Figure 14**. A website that is trustworthy will be flagged green.

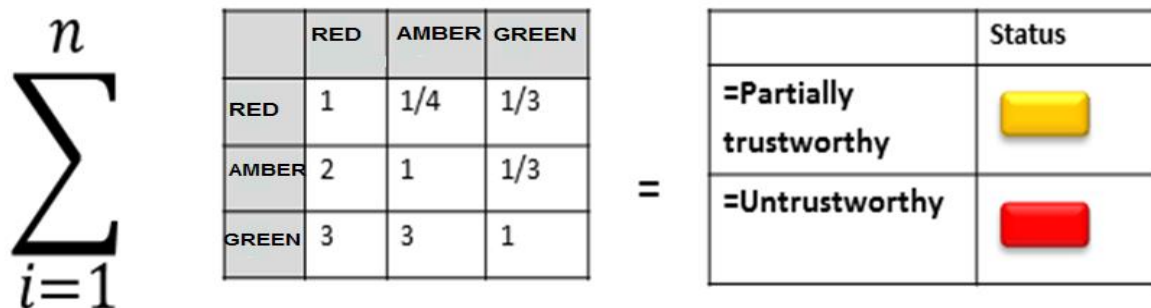
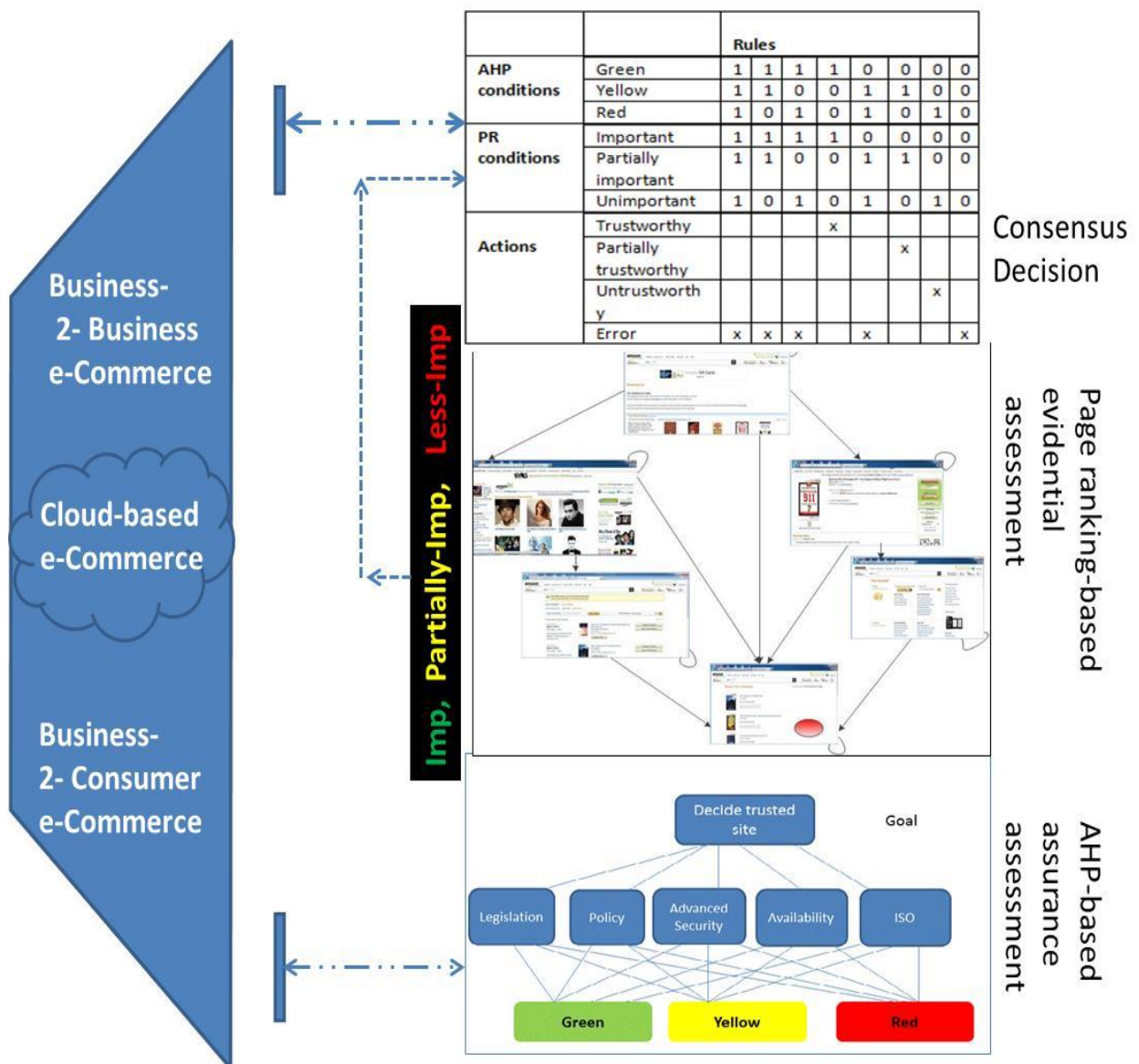


Figure 14: Objective function (see online version for colours)

### 3.5 DEVELOPMENT OF THE PROPOSED PRAHP INTELLIGENT E-COMMERCE ASSURANCE MODEL

#### 3.5.1 Establishing a framework of intelligent e-commerce assurance

The model has been divided into three segments: bottom up, analytical hierarchy assessment, which is complemented by evidential reasoning of PR, which is in turn supplemented by the guidance of the decision table to come to a consensus decision. The model is suitable for use by various e-commerce market types, i.e. B2B, B2C, cloud-based e-commerce environments etc.



**Figure 15: The development of PRAHP model**

In a nutshell, the construction of the PRAHP model is depicted in **Figure 15**, where the working of the AHP and PR is fused together to reach consensus on the trustworthiness of an e-commerce website.

The selection of attributes was guided by the ISO 27001/27002 standards backed by literature review and statistical assessment [97][98]. The ISO 27001 is a best practice standard for a well-governed and established information security management system. It covers various domains, which must be included in an effective information security management system (ISMS). It also provides a list of controls in annexure A of the standard that must be considered when implementing effective ISMS in electronic environments.

Some of the controls identified in the ISO 27001 standard [98], which relate to the online environment, were used as attributes for this study: availability of information processing, compliance with legal regulation, secure logon, policy and compliance to standards. These were the controls where the attributes of PRAHP were culled for the purposes of this study as availability (A), adaptive legislation (AL), advanced security logon (AS) and adaptive ISO standards (AI).

The attributes of the model will be explained in greater detail in subsequent sections.

#### *3.5.1.1 Adaptive legislation (AL) as an assurance measure*

The nature of the e-commerce environment is much more complex compared to the brick and mortar environment. This is promulgated by many factors, such as the virtual nature of e-commerce platforms, where the transacting parties do not necessarily have any face-to-face interaction.

In the event of cybercrime, where for instance a customer's personal information can be leaked owing to an information security compromise in a cloud-based e-commerce environment, it would be difficult to establish which laws are applicable in such an event.

In South Africa the Electronic Communications and Transaction (ECT) Act [99] is used to regulate internet and e-commerce related matters to a certain extent, as it outlines the requirements for online vendors.

Different electronic retailers (e-tailers) are governed by various laws based on the country from which they physically operate. The issue of legal jurisdiction in the event of an e-commerce breach can be problematic if the parties affected reside in different countries and the perpetrators reside elsewhere. However, legislation remains important with regard to the trustworthiness of a website. Hence, a website such as Bidorbuy [100], which is an example of a B2C, refer to the South African Protection of Personal Information Act, no. 4 of 2013, to give assurance to customers regarding the protection of their personal information.

Based on the importance of legislation in e-commerce transacting, legislation has been identified as a key attribute that must be included in the development of PRAHP. In the uncertain world of e-commerce, users feel unsafe if they do not know which laws will be used in the event of fraud being committed.

### *3.5.1.2 Adaptive ISO (AI) standard as an assurance measure*

Various best practice standards have been developed to standardise certain ways of doing things, such as ways of developing certain products or the configuration of certain requirements. Examples of some of the standards' bodies are the American National Standards Institute and the ISO.

In the e-commerce context, the ISO [101] security standard poses certain requirements that must be met in order to be certified as a secure e-commerce transacting platform. For e-commerce markets an ISO certification assures customers and partners that the transacting platform and associated processes can be trusted. Amazon [33] is an example of a B2B and B2C e-commerce store with an ISO seal that gives customers assurance concerning the safety of the transacting site.

Compliance with best practice standards is important for many organisations, particularly for organisations that aim to stand out and differentiate themselves from others. In an e-commerce environment where sales of various products take place, in order for users to trust the quality of products, compliance with quality standards such as the ISO 9001 would provide a reasonable level of assurance that the products sold are of good quality, as the manufacturer adheres to best practice measures to develop the product. In an e-commerce environment where security threats are prevalent, it is paramount for an online vendor to comply with best practice standards such as the ISO 27002 security standard. It is for that reason that the ISO 9001 standards were identified as important assurance measures of trustworthiness. The ISO standard consists of a set of requirements that must be met in order to have a reliable quality management system.

An example of an e-commerce vendor that has attained ISO certification numerous times is IBM [35].

The certification has been issued to specific departments and other regional businesses per country.

### *3.5.1.3 Policy (P) as an assurance measure*

Policies have been used by various business organisations in the brick and mortar environment to communicate management's intention to manage certain processes in an organisation in a particular manner. For instance, many business organisations, as well as various government departments, have information security policies that govern the use of information in the organisation. An example of a governmental institution with an information security policy is the Municipality of BelaBela[102]. An organisation that has an information security policy aims to protect both the users of information and the organisation itself from information security breaches.

Policies have been extended to online environments in order to provide assurance on various aspects involved in online transacting. Many online stores have compiled policies in an attempt to provide assurance on matters such as the protection and privacy of customer information. Examples of online stores that have various policy statements displayed on their websites include Fashion Hub[103], My Car [104] and Cape Coffee Beans [105].

It is quite obvious that customers gain trust in the e-commerce website when they read policy statements providing guidance on the action that will be taken in an unfortunate event.

For instance, customers may want to read a refund policy to find out how they will be refunded in the event of an order cancellation. The presence of relevant and up-to-date policies on an e-commerce site gives assurance to customers about the trustworthiness of a website.

### *3.5.1.4 Advanced user security (AS) login as an assurance measure*

In an effort to create a secure transacting platform in e-commerce environments, an online account must be created following registration. Different online stores require different information in order for the account to be created and most of the required information is personal customer information such as names, addresses and in certain instances credit card information.

The login credentials required are user name and password, such as the ones generated in [106]. The merits of having secure login are that personal information is secure and protected from malicious attacks. However, if the login details are weak and consequently easily guessable, they will fail to provide the desired adequate security. Another factor that can

potentially weaken the strength of security controls is an e-commerce website with a functionality that allows users to stay signed in. The risk of choosing such a functionality is that a computer that is shared or stolen becomes vulnerable to unauthorised access by attackers.

An e-commerce website that requires a user to register using strong credentials is more likely to gain trust from both novice and expert users than a website requiring weak login credentials or none. Websites that exhibit stronger logical access security controls provide assurance concerning the security trustworthiness of the website, particularly if there is a history of hacking. Webstore [53] is an example of a B2B e-commerce site that offers strong security login requirements using unique login credentials.

#### *3.5.1.5 Site availability (A) as an assurance measure*

Unlike in the brick and mortar environment where the unavailability of a store can be physically verified, it is quite difficult in the online environment to determine if a store is constantly available or not. Customers are generally reluctant to buy online services or goods on a website that is constantly unavailable. Continuous availability of a website is an important security measure.

One of the benefits that e-commerce markets have over brick and mortar environments is their ability to operate constantly, which attests directly to the availability of products and services through their websites. The information security principles based on the ISO 27001 security standard entail confidentiality, integrity and availability of information.

Technical tools for monitoring purposes have been developed and continue to be developed to provide information on the availability of websites to provide assurance to customers in that area.

Various tools are used to check for the availability of websites. Site 24x7 [107] is an example of a website that provides information on the availability of information on various sites. The reliability of the information provided in freely available tools on the internet requires further investigation.

### 3.5.2 PRAHP mathematical and algorithmic analysis

#### 3.5.2.1 Phase 1: Constructing paired comparison matrix level 1 with respect to (wrt) e-commerce assurance goal

In determining the trustworthiness level of an e-commerce site, the AHP requires the construction of a pairwise comparison matrix as the first step. This matrix is depicted in step 1, Paradigm 1, which shows a comparison of the five identified assurance attributes, i.e. P, AS, A, AI and AL. In an e-commerce environment an assessment is done based on AHP to determine the trustworthiness of the site, taking into account the five attributes. The strong presence of a particular attribute signifies the level of importance of that attribute on the website as an assurance measure. The pairwise comparison is constructed with respect to the goal.

A real e-commerce website A was used for the assessment of the attributes. For instance, the P attribute was assessed in relation to other attributes, i.e. ISO standards, to determine which attribute demonstrated the higher level of trust compared to the others. The AHP paradigm 1 for the pairwise comparison with respect to the goal is illustrated in steps 1- 6.

#### **Paradigm 1- AHP module of PRAHP model with respect to the goal**

**Step 1:** Construct a paired comparison matrix wrt to the goal.

This step shows the comparison matrix for website A. The attributes that are compared in this pairwise comparison matrix are AL, P, AS, A and AI and these are compared with respect to the goal.

From data parameters captured from a website, compare each pair of attributes (e.g. AL, P) for dominance.

Assess which attribute the site counts as more important and the extent of its importance.



$A_{ij} =$

	AL	P	AS	A	AI
AL	1	1/3	1/5	7	9
P	3	1	3	5	7
AS	5	1/3	1	9	3
A	1/7	1/5	1/9	1	3
AI	1/9	1/7	1/3	1/3	1

**Step 2:** Reciprocal matrix:

$$a_{ji} = \frac{1}{a_{ij}}$$

A stands for the comparison matrix A,  $A_{ji}$  = where j is the element of row j and column i.

**Step 3:** Normalise the matrix in step 2 by dividing each element by the column sum  $S_1, S_2$ , etc.

$$S_j = \sum_{i=1}^n A_{ij}$$

$$A' = \frac{1}{n} \begin{bmatrix} A_{11}/S_1 & \dots & A_{1j}/S_j \\ \vdots & \vdots & \vdots \\ A_{i1}/S_1 & \dots & A_{ij}/S_j \end{bmatrix}$$

**Step 4:** For normalised principal eigenvector V, average across rows, i.e. each row added and then divided by n (say n=5):

$$V_j = \frac{1}{n} \begin{bmatrix} A'_{11} + \dots + A'_{1j} \\ A'_{i1} + \dots + A'_{ij} \end{bmatrix} \times 100\%.$$

**Step 5:** In order to check the consistency of the observations using eigenvalue, compute:

$$\lambda_{\max} = S_1(V_1) + S_2(V_2) + \dots + S_j(V_j) .$$

If  $\lambda_{\max} \approx n$ , then  $A_{ij}$  is consistent.

**Step 6:** Deviation of consistency is computed using the consistency index (CI):

$$CI = \frac{\lambda_{\max} - n}{n - 1} .$$

By deduction from the consistency ratio, if  $(CI < 0.1)$ , then  $A_{ij}$  is consistent.

### 3.5.2.2 Phase 2: Constructing paired comparison matrix level 2 in relation to level 1

The level 2 indicators that have been selected for the comparison matrix are red (R), amber (A) and green (G). A paired comparison matrix is based on the assessment of the three indicators in relation to level 1 attributes, i.e. AS, P, A, AI, AL. In a website where it must be determined whether it is secure or not secure, it will be marked by either the green colour (for the most secure) or the red for the least secure. The sum of the indicators adds up to 100%, which constitutes level 2 indicators.

#### Paradigm 2 - AHP module of PRAHP model with respect to level 1

**Step 1:** Construct a paired comparison matrix level 2 wrt level 1.


From data parameters captured from a website, compare each pair of indicators (e.g. R, G) in relation to a level 1 attribute.

Assess which indicator is more likely to be important and the extent of its importance using

**Figure 18.**

**Step 2:** For reciprocal matrix:

		R	A	G
A <sub>ij</sub> =	R	1	1/2	1/3
	A	2	2	3
	G	3	3	1

$A_{ij} = 1/A_{ji}$ 


**Step 3:** Normalise the matrix in step 2 by dividing each element by the column sum  $S_1, S_2$ , etc.

$$S_j = \sum_{i=1}^n A_{ij}$$

$$A' = \frac{1}{n} \begin{bmatrix} A_{11}/S_1 & \dots & A_{1j}/S_j \\ \vdots & \vdots & \vdots \\ A_{i1}/S_1 & \dots & A_{ij}/S_j \end{bmatrix}$$

**Step 4:** For normalised principal eigenvector  $V$ , average across rows, i.e. each row added and then divided by  $n$  (say  $n = 3$ ):

$$V_j = \frac{1}{n} \begin{bmatrix} A'_{11} + \dots + A'_{1j} \\ A'_{i1} + \dots + A'_{ij} \end{bmatrix} \times 100\%.$$

**Step 5:** Repeat steps 5 and 6 in paradigm 1.

Real-life data continues to be used for assessment purposes in paradigm 2. The pairwise comparison of the assurance indicators, in relation to the level 1 attribute, e.g. ISO, is illustrated in paradigm 2 and the only exception is that  $n = 3$  instead of 5.

### 3.5.2.3 Phase 3: Emergence of overall composite matrix for the assurance indicators

Based on the AHP assessment, the results of level 1 and 2 assessments provide the overall website rating. The final website rating based on AHP is achieved through the combination of level 1 and 2 attribute assessment.

Equations (4)-(6) are used for the normalisation of linear combinations of multiplication between weights and priority vectors in order to obtain composite vectors.

$$\text{Green} = (W_{L1}L * V_{L2}L) + (W_{L1}A * V_{L2}A) + \dots = V_1\% \quad \dots\dots\dots (4)$$

$$\text{Amber} = (W_{L1}L * V_{L2}L) + (W_{L1}A * V_{L2}A) + \dots = V_2\% \quad \dots\dots\dots (5)$$

$$\text{Red} = (W_{L1}L * V_{L2}L) + (W_{L1}A * V_{L2}A) + \dots = V_3\% \quad \dots\dots\dots (6)$$

where

$W_{L1}$  = Weight from level 1 matrix,  $V_{L2}$  = Vector from level 2 matrix.

Based on the composite vector equation, the results of the RAG status show the percentage ratings from the PRAHP first modular technique.

### 3.5.2.4 Phase 4: Preparing evidence from Page ranking for cooperation

The PR technique is the second leg of the PRAHP model. The AHP is complemented by the PR technique. The input in the PR technique consists of an evaluation of e-commerce sites' links, i.e. inbound/outbound. The final output of PR is the value as a percentage of importance. In terms of the steps shown in paradigm 3, step 1 demonstrates how the binary link matrix is constructed; the computation of outbound links per column is shown in step 2. The matrix is then normalised through the damping factor and sum product values in order to get the next PR value; this is shown in steps 3-6. Convergence is reached after numerous iterations of step 7, in paradigm 3.

#### **Paradigm 3: Complementary PR module in PRAHP model**

**Step 1:** From data parameters captured from websites, construct a binary link matrix  $L_{ij}$ ,

$$L_{ij} = \begin{cases} \text{If } page\ j \rightarrow page\ i, & L_{ij} = 1 \\ \text{otherwise} & , \quad zero \end{cases}.$$

**Step 2:** Compute the number of outbound links  $C_j$  per column:

$$C_j = \sum_{i=1}^N L_{ij}.$$

**Step 3:** Compute to normalise the link matrix in step 2 as:

$$\frac{L_{ij}}{C_j}.$$

**Step 4:** Set initial value of PR as number of outbound links:

$$P_j = C_j.$$

**Step 5:** Compute the sum product for each row as:

$$\sum_{i=1}^N \left( \frac{L_{ij}}{C_j} \right) P_j.$$

**Step 6:** Set the value of damping factor  $d$ , e.g. 0.85.

**Step 7:** Compute the next value of PR as:

$$P_i = (1 - d) + d \sum_{i=1}^N \left( \frac{L_{ij}}{C_j} \right) P_j.$$

**Step 8:** Iterate step 7 until convergence, i.e.

$$P_i \cong P_j.$$

**Step 9:** Rank  $P_i$  and categorise into the number of indicators in AHP.

#### 3.5.2.5 Phase 5: Combining and deriving a consensus decision on cloud assurance

This section demonstrates how AHP and PR techniques are combined in order to come up with a final PRAHP website rating, which ultimately shows the final EAR for an e-commerce environment.

To reach an inclusive final decision on the trustworthiness of an e-commerce website, the  $P_i$  results are combined with step 3 of paradigm 2 of the AHP module using the principles of a decision table. This results in the following equation, where the outcome is trustworthy (T), partially trustworthy (PT) or untrustworthy (UT), as shown in equation (7):

$$\left. \begin{array}{l} \text{Site A} = \text{PR}(P_1) + \text{AHP}(V_1) = \{T, PT \text{ or } UT\} \\ \text{Site B} = \text{PR}(P_2) + \text{AHP}(V_2) = \{T, PT \text{ or } UT\} \\ \dots\dots = \dots\dots + \dots\dots = \dots\dots\dots \\ \text{Site N} = \text{PR}(P_i) + \text{AHP}(V_i) = \{T, PT \text{ or } UT\} \end{array} \right\} \quad (7)$$

### 3.6 EVALUATION AND VALIDATION MECHANISM

In this study different techniques were used to assess and validate the collected data in order to interpret it and obtain the necessary results to conclude the study. This section is aimed at discussing the evaluation methods that were used in the study, specifically the quantitative and qualitative methods. Besides the consistency, accuracy and validation metrics in AHP and PR presented in the preceding sections, the following sections complement the evaluation mechanism.

#### 3.6.1 Trustworthy accuracy

Cyber threats make buying online risky, considering the fact that some sites are more untrustworthy than others. It is therefore pertinent to have a mechanism that warns customers about the trustworthiness of a website before they commit their payment information, to assist them in making informed purchasing decisions.

Some of the benefits that come with having a mechanism of informing customers of the trustworthiness of a website include the following:

Customers will not easily fall victim to cybercrime in the form of theft of payment details as a result of transacting from untrustworthy websites.

In many instances when buying goods and services online, privacy of information and security of information can easily be compromised if a website is rated untrustworthy.

Alerting users regarding the trustworthiness or untrustworthiness of an e-commerce website is useful in assisting them to prevent falling victim to malicious attacks.

In this study the trustworthiness, partial trustworthiness and untrustworthiness accuracies of websites are calculated as follows:

Trustworthiness accuracy = (number of trusted sites/total number of sites) X100%

Partially trustworthiness accuracy = (number of partially trusted site/total number of sites) X100 %

Untrustworthy accuracy = (Number of untrustworthy sites/total number of sites) X100 %.

These accuracies are validated in section 3.6.2.

### **3.6.2 Qualitative customer validation**

In e-commerce environments where the buying and selling of goods and services occur virtually online, most consumers are reliant on consumer reviews of a website or a product.

The reviews are in different forms; consumers can simply use a “thumb up” sign for excellent service or a “thumb down” sign for poor service, which is usually accompanied by a comment or a rating scale from 1 to 5 where poor is 1 and excellent is 5. On certain websites, the users only have an option of capturing a compliment or a complaint.

The number of consumers who read and trust the online consumer reviews is said to be increasing [108] and these reviews do influence customers’ buying behaviour.

Customers can use different methods to provide feedback on their online purchasing experience, i.e. they can post a complaint or a compliment directly on a vendor website, they can provide feedback by posting on other third-party websites or they can simply speak about the issue to other people informally. Customer feedback has been seen as an excellent mechanism of identifying areas for improvement.

Customer reviews of the online shopping experience and product quality are important for customers, because they are dependent on such reviews to decide whether to buy that product or to buy from that particular website [109] .

### 3.6.3 Statistical hypothesis

A hypothesis is a prediction based on limited or no evidence, with the intention of expanding on it for further investigation. A hypothesis usually comes after the research question. A hypothesis normally starts with “if”, followed by a “then” or “ else” statement, e.g. if inbound links are increasing, then the reliability of a website increases [110]. The null hypothesis would be “inbound links decrease the reliability of a website”. Once the null hypothesis is rejected, then the alternative hypothesis holds.

In this study, the hypothesis was testable by the survey of articles that was done.

Formulation of a hypothesis required the following steps:

Variables that needed to be used had to be identified, e.g.  $H_0$  and  $H_1$ , where for instance the null hypothesis is  $H_0$  and the alternative hypothesis is  $H_1$ .

A population size was determined based on the number of e-commerce journals reviewed. Based on the population, a sample of e-commerce articles was selected.

For example, hypothesis testing was done to determine the association of assurance attributes with the assurance measures detailed below:

$H_0^1$ : *The level of adaptive legislation of a country is not positively associated with other assurance measures.*

$H_0^2$ : *The level of adaptive ISO standards and other assurance measures is negatively associated.*

$H_0^3$ : *The level of policies of a business enterprise does not positively influence other assurance measures.*

$H_0^4$ : *The level of strength of advanced user security does not influence other assurance measures.*

$H_0^5$ : *The level of e-commerce site availability and other assurance measures are negatively associated.*

### 3.7 PRAHP DEPLOYMENT SCENARIO

The scenarios below demonstrate how PRAHP will be used to signal a trustworthy and untrustworthy website to the customer.

#### 3.7.1 Trustworthy e-commerce website

The conventional buying of goods and services online requires the creation of a user account by means of a username and password. Once the account has been created, a user will be able to buy online and provide his or her payment details to conclude the order. In terms of the conventional transacting platform, there is seldom any direct alert, which cautions whether the website is trustworthy or untrustworthy before customers can supply their payment details, such as credit card information. In order to alert a customer to the trustworthiness of a website, PRAHP has some controls to that effect.

As depicted in **Figure 16**, Jasmine is intending to buy a dress on the online store for her daughter's birthday. She simply logs into the website by supplying her user name, password and a uniquely generated pin. She then proceeds to add the dress that she is planning to buy and then goes to check out, but before checkout a green message flashes at the bottom of the screen, which notifies her that the website is safe to transact from. She proceeds with capturing her credit card details for checkout purposes, concludes the transaction and then awaits the delivery of the dress.

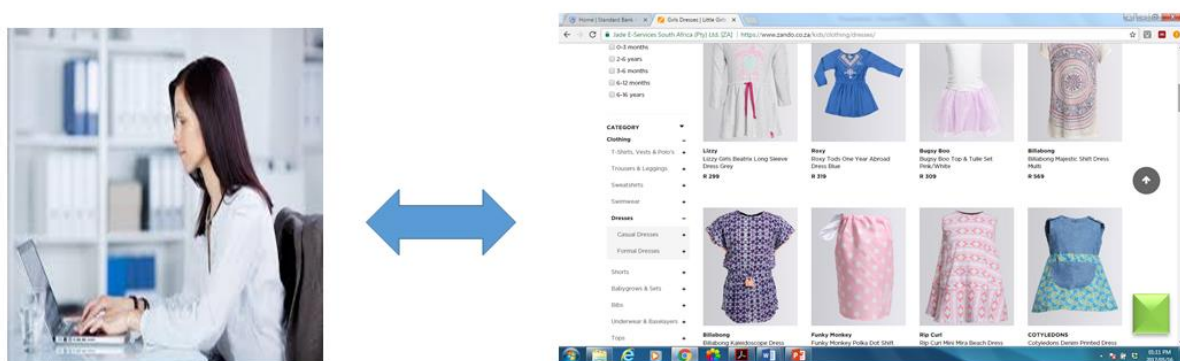


Figure 16: Trustworthy website



### 3.7.2 Untrustworthy e-commerce website

In e-commerce environments, there are websites that are trustworthy and those that are not. Some of the trustworthy websites are the secure websites that are followed by an “s” for secure after typing “https”; in a conventional unsafe website, a customer would not be warned beforehand about the unsafe nature of the website. Some tools, such as the McAfee Secure [46] web advisor, do attempt to warn their users regarding the safety of a website, i.e. whether it is a high-risk site or not. The risk ratings are based on the website’s reputation, but other factors that are taken into consideration are not necessarily disclosed. PRAHP has been designed to alert the user to the untrustworthiness of the website by taking into account availability, security, compliance with best practice standards and legislation and the existence of relevant policies.

**Figure 17** depicts how PRAHP can alert transacting customers when a website is untrustworthy. In a C2C e-commerce environment where a customer, Joseph, sees an advertisement of a car on sale with a nice picture of the car at a reasonable price, he is tempted to buy. As soon as Joseph sees a list of options to choose from in order to secure his purchase, he quickly selects the “ I’m interested, please contact me” option, and soon thereafter a red button appears, informing him that it is an untrustworthy website. He is offered an option to continue or exit the site before divulging further personal information.



**Figure 17: Untrustworthy Website**

PRAHP is useful in alerting users regarding the trustworthiness of a website before they commit their payment details.

### **3.8 CHAPTER SUMMARY**

This chapter gave an outline of the research method that was used in this study. The data collection methods that were used, namely the website analysis, literature review and statistical analysis, were discussed in detail in sections 3.2 and 3.3. The mathematical illustrations of the objective functions and notations applied in this study were also outlined.

The aim was to scrutinise the method of resolving the identified research problems through PRAHP. The framework for e-commerce assurance provided a description and reason for the selection of the five attributes that have been selected for assurance evaluation for an e-commerce website. The framework comprises the following attributes: AL, AI, A, P and AS.

The mathematical and algorithmic analysis of PRAHP was discussed in section 3.5.2 outlining all the steps from the construction of a pairwise comparison matrix to reaching a consensus decision on e-commerce assurance. The research study's evaluation and validation methods were also discussed. The final picture or view in terms of how PRAHP will be deployed to show the trustworthy or untrustworthy scenario was highlighted in section 3.7.

This research develops a new methodology, which is applied to address societal problems intended to have a socio-economic impact. This chapter discussed all the artefacts of the model, the techniques and approaches and how they are fused to give trustworthiness assurance on an e-commerce website.

# CHAPTER 4 – EXPERIMENTAL EVALUATIONS AND RESULTS

## 4.1 OVERALL EXPERIMENTAL SETUP

The experiments conducted using PRAHP are explained in detail in sections 4.3 to 4.6 respectively. This section introduces the overall experimental setup that was applied in the different types of e-commerce market experiments.

Ten e-commerce sites were used for each PRAHP experiment in this study, i.e. cloud-based e-commerce, B2B and B2C e-commerce and general e-commerce sites. As the intention of this study was to experiment on different e-commerce markets and see PRAHP's results, the number of websites was limited to only 10 websites per experiment, which resulted in a total of 30 websites for the three experiments conducted. This was done to permit detailed analysis of a particular website using PRAHP, as trust is fundamental on all e-commerce websites.

These websites are real and in production. The criteria for website selection are detailed in the subsequent sections. In all experiments, pseudonyms of websites were used for confidentiality reasons. In order to bring context to the websites used, a description of the websites has been added to illustrate the type of services offered by the particular website.

The literature survey and the assessment of challenges faced by cloud-based e-commerce websites, general e-commerce websites, B2B and B2C e-commerce websites guided the selection of attributes (AL, AI, A, AS, P) used in these experiments. In all the experiments, the attributes were assessed based on the macro-based AHP assessment tool [96]. This tool allows for the capturing of attributes and assignment of relevant weights using the scale shown in Figure 18. The duration of the experiments was from 2014 until 2016.

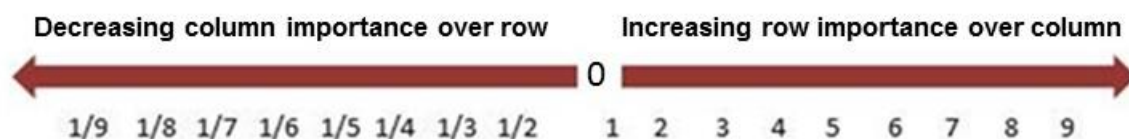


Figure 18: AHP weighting scale

For **Figure 18**, it is assumed that the attribute AL is significantly more important than A; then in terms of the value that would be assigned to AL according to this scale it would be on the far right, e.g. 6, in which case the inverse would be 1/6. In short,  $AL/A = A/AL$ ;  $6/1 = 1/6$ . In order to ensure the reliability of the weightings and to be objective, real-life data from the websites was used.

These rating scales are in percentage form and the sum total of these percentages for each of the five attributes add up to 100%. The results constitute level 1 vectors.

The next section is an experiment that was conducted to identify e-commerce assurance models' weaknesses.

## **4.2. EXPERIMENT 1: ANALYSIS OF E-COMMERCE ASSURANCE MODELS AND PRAHP ATTRIBUTES**

### **4.2.1. Introduction**

As the foundation for the experiments that are carried out in this chapter, relevant e-commerce literature was reviewed that uncovered the strengths and most importantly, the weaknesses of the existing e-commerce assurance models. The aim was to propose a model that seeks to address some of those weaknesses. These weaknesses are identified and explained in section 4.2.3. A proposal for an e-commerce assurance framework is shown in **Figure 19**. The model consists of the attributes, i.e. AL, AI, AS, P and A, which are discussed in experiments reported in section 4.2.3(a)-4.2.3(e).

The work described in section 4.2 forms the basis for the experiments in sections 4.3 to 4.6.

### **4.2.2. Statistical survey on assurance model weaknesses**

This section discusses the different types of e-commerce assurance models, how these models are perceived in terms of trustworthiness levels in the literature reviewed on web assurance and how trustworthy some of the e-commerce assurance models are. The following issues were noted:

High information quality seals were found to be more trustworthy in comparison to low information quality seals [111], [112], [113]. Examples of high information quality seals include the WebTrust and SysTrust seals. The challenge with high-quality seals is that they are not interactive, nor do they include consumer input. An example of a low information quality seal is the VeriSign seal. The advantage of a low information quality seal is that it provides assurance on a specific aspect only, e.g. security.

A survey of weaknesses has been conducted, as discussed in section 2.2.6, and this forms the basis of attribute selection.

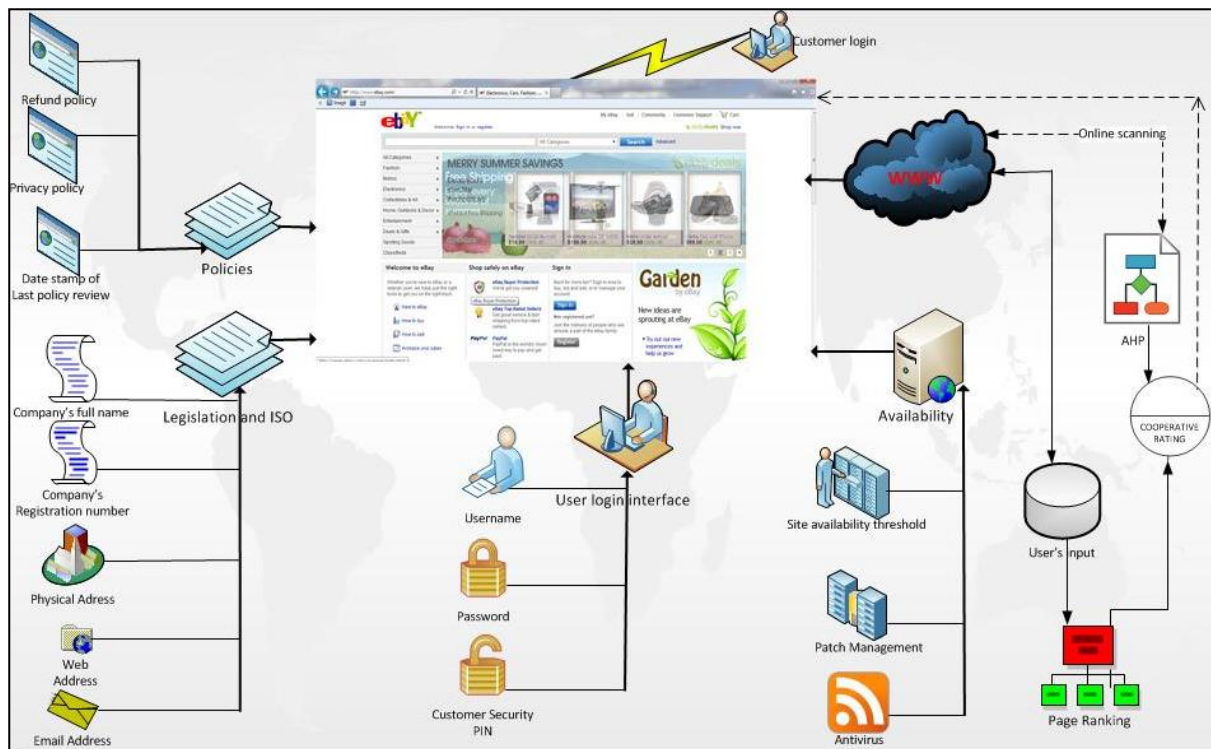
#### **4.2.3 Statistical analysis on assurance attribute selection**

The e-commerce assurance model aims to provide useful information for decision-making to a customer concerning the website's trustworthiness. **Figure 19** shows the proposed e-commerce assurance model, which aims to provide trustworthiness assurance by addressing the shortcomings of the existing e-commerce assurance models.

In order to transact from a website, the proposed model in **Figure 19** requires a customer to create an online account for transacting purposes with an online vendor. A strong user name, password and customer-selected pin will be required to authenticate the user. After logging in, a customer will be asked a few questions through a short survey, to determine if the customer has read the privacy policy and refund policy on the site and secondly if the customer has experienced a bad or good shopping encounter through the website or not.

The model will aggregate the user's input. In addition to the user's input, the model consists of the following attributes: policies, legislation, advanced security login, availability and ISO standards. The model will test the presence of the policies and the last policy review date to determine its currency, and based on the results of the analysis it will award a rating. Furthermore, the model will check for compliance with South African ECT legislation, specifically on the provisions relating to an e-commerce website, and will rate the level of compliance of the site. Adoption of the ISO standard, specifically the ISO 27001, will be confirmed by the model on the security of online transactions, specifically encryption.

An online scan to determine if the website is consistently available and has the latest anti-virus software and latest patches will be done to ensure that it is not vulnerable to online attacks. The model will combine all the attribute information using the cooperative rating based on AHP and PR to strengthen the assurance level. If the site is trustworthy, a green flashing circle will be displayed and if the site is unsafe to transact from, a red flashing circle will be displayed. These ratings will assist the customer to decide whether to continue with an online purchase or to abandon the online purchase. Unlike many e-commerce assurance models that do not require customer input or legislation compliance, this model goes a long way in providing reliable assurance concerning website trustworthiness.



**Figure 19: Framework of PRAHP Assurance model selection**

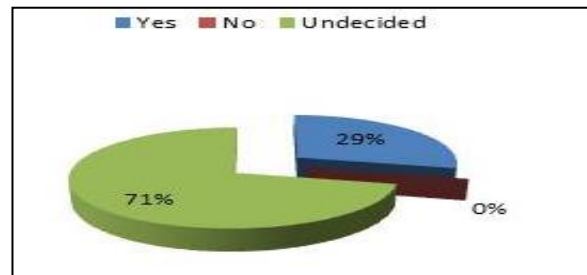
The detailed discussions of the model attributes are presented in section points (a) to (e) of section 4.2.3. One can see that the proposed model has more advantages than the existing ones. In order to back up the importance of an attribute, a survey was conducted for every attribute in an attempt to determine its importance as mentioned or discussed in the existing literature. Different sample sizes were used based on this experiment. The relevance of the different sample sizes is an indication of the availability of literature that covers a particular attribute. Bigger samples were used where there was more literature to use and smaller samples were used for attributes that have not been covered much in the literature.

#### **a) Adaptive legislation as an assurance measure**

Different countries have different e-commerce legislation, which can be used with the model. For the purposes of this study the South African ECT legislation will be used, because it is specific to the requirements of e-commerce environments. The South African ECT Act (2002) contains certain provisions, which must be catered for by online vendors. An online vendor must comply with the ECT Act's provisions, which are pertinent to the nature of services offered. The specific provisions are as follows: a) full name and legal status; b)

physical address; c) website address and e-mail address; d) The physical address where that vendor will receive legal service of documents. Because of the importance of these provisions of the ECT, it would be worthwhile to include these provisions so that they can cooperatively constitute a trustworthy measure on the proposed model.

The model will check for the existence of this required information on the website and produce an average rating combined with the other attributes.



**Figure 20: Is legislation an assurance measure?**

**Figure 20** was produced by conducting a survey of 28 journal articles from the IEEE and Science Direct databases. When selecting the sampling frame in October 2012, some of the following keywords were used: legislation, regulation, acts, assurance, web, seals, e-commerce, assurance, model. The sample of articles was chosen based on their relevance to the subject of this study, where the aim was to determine the number of articles that supported the notion that legislation is an assurance measure.

Of the 28 sampled journal articles, 71% were undecided and 29% found legislation to be an assurance measure [114][115]. In order to encourage online consumer confidence in e-commerce, a secure legislative framework is recommended [118]. No articles cited legislation as an untrustworthy measure. These results support this research's objective.

### **(b) Adaptive ISO standards as an assurance measure**

The ISO 27002 standard is regarded as the e-commerce international benchmarking standard for information security [116]. Some of the e-commerce requirements from the ISO 27001 standard are likely to enhance the assurance provided by the proposed model. The ISO has developed and continues to develop various standards in the ICT field.

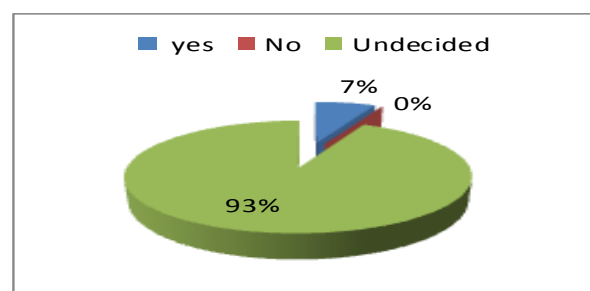
These standards are very useful because of their relevance and guidance on how to manage various ICT environments and systems well. The ISO 27002/27001 are some of the

information security standards that provide guidelines to organisations and practitioners on how to secure management systems.

E-commerce is also covered in the ISO 27001 in terms of how it should be secured best. Below is a summary of the recommendations on the ISO 27001 (South African National Standard, 2005); Section A.10.9 requires that the following controls be applied in the e-commerce environment:

- A.10.9.1 Information involved in electronic commerce passing over public networks shall be protected from fraudulent activity, contract dispute, and unauthorised disclosure and modification.
- A.10.9.2 Information involved in on-line transactions shall be protected to prevent incomplete transmission, misrouting, unauthorised message alteration, unauthorised disclosure, unauthorised message duplication or replay.
- A.10.9.3 The integrity of information being made available on a publicly available system shall be protected to prevent unauthorised modification.

This section of the standard was identified as vital for inclusion in the proposed model. The proposed model checks for encrypted transactions on the website. This check, together with the other attributes, will be assessed and aggregated in order to show the final website score/rating. To determine if there is literature referring to legislation and ISO standards in general as a trustworthiness measure, a survey of articles was conducted and the results of the survey are shown in **Figure 21**.



**Figure 21: Are ISO standards an assurance measure?**

**Figure 21** was produced by conducting a survey of 15 journal articles from the IEEE and Science Direct databases.

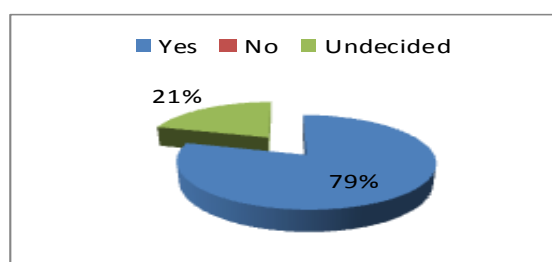
When selecting the sampling frame in October 2012, some of the following keywords were used: Standards, ISO, trustworthiness, assurance, web, seals, e-commerce, assurance and model. The sample of articles was chosen based on their relevance to the subject of this study,



where the aim was to determine the number of articles stating that ISO standards are an assurance measure. Of the 15 sampled journals, 93% of the articles were undecided and 7% found ISO standards to be an assurance measure, which supports the proposed assurance model.

### **(c) Policy as an assurance measure**

Policies have often been used by the various websites to provide assurance to prospective customers concerning the privacy of information and other related practices. In terms of the South African ECT Act, certain policies are required by law to be displayed on vendor websites. These include policies such as privacy and refund policies, which must appear on the online vendor's site. Displaying policies on a website is critical, so that consumers can know and understand how their personal information will be handled in terms of privacy. In order to determine within the e-commerce assurance literature and related fields whether the policy is viewed as a trustworthiness measure, a survey was conducted and the results are displayed in **Figure 22**.



**Figure 22: Is policy an assurance measure?**

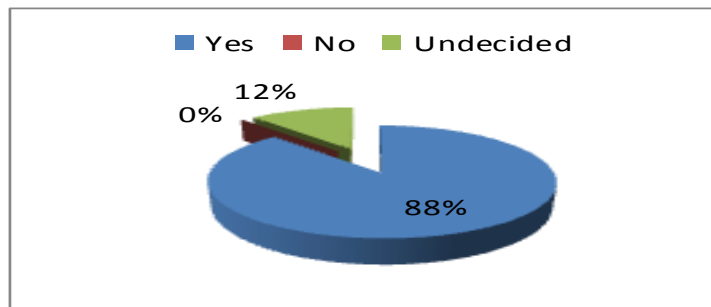
A survey of 30 journals was conducted from IEEE and Science Direct databases. When selecting the sampling frame in October 2012, some of the following keywords were used: policy, trustworthiness, assurance, web, seals, e-commerce, assurance and model. The aim was to determine the number of articles that viewed policies as an important assurance measure [10][117][118]. The survey results revealed that 79% of the articles viewed policies as an assurance measure, which supports the view of the proposed model. In 21% of the articles, policy was not directly or by implication stated as an assurance measure.

### **(d) Advanced user security login as an assurance measure**

Security of information is crucial in an e-commerce environment. Customers often need to be assured that their online payments are secure in an online environment. Security of information

starts when logging into a system and continues throughout the processing of the transaction information, where strong encryption methods must be used. Security of transactions in an online environment is therefore vital to encourage online customer trust.

**Figure 23** shows the results concerning how security of information in a transacting environment is perceived, whether it is seen as a trustworthy measure or not.



**Figure 23: Is advanced user security an assurance measure?**

A survey of 25 journals from the IEEE and Science Direct databases was conducted. When selecting the sampling frame in October 2012, some of the following keywords were used: user, security, login, credentials, trustworthiness, assurance, web, seals, e-commerce, assurance and model. The aim was to determine the number of articles that viewed security of transactions as an important measure of trustworthiness. Based on previous reviews users are not comfortable to transact via the internet unless they are comfortable with the security of their online transactions [18][113]. Assurance on security to online customers encourages adoption of the method [119].

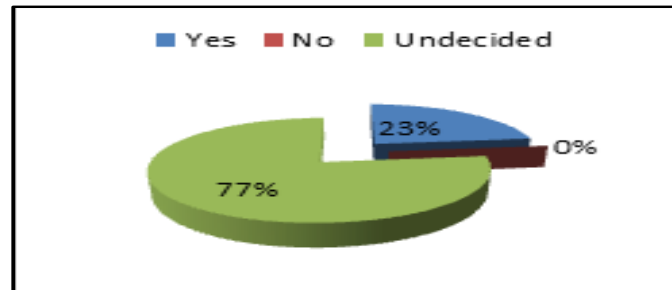
The results revealed that 88% of the articles viewed security as an assurance measure, 0% objected and 12% were undecided. The results generally support security as an assurance measure, which clearly supports the view of the proposed model. The articles were not descriptive in terms of differentiating between advanced user security logon and security, but they referred to security of online transactions as an assurance measure.

#### **(e) Site availability as an assurance measure**

The constant availability of a website is important in establishing and maintaining online trust. A website that is constantly unavailable could make users suspect that the online vendor's store is unreliable. Availability of systems is often affected by factors such as poor patch management or lack of the latest antivirus software, which could render the site vulnerable to online attacks.

Availability is an attribute that is least recognised within the web seal industry when compared to policies, security and legislation.

In order to determine the number of researchers who viewed availability as an assurance measure, a survey was conducted and the results are displayed in **Figure 24**.



**Figure 24: Is site availability an assurance measure?**

Website availability is an attribute that is seldom discussed in e-commerce literature on web assurance. A survey of 30 journals from the IEEE and Science Direct databases was conducted. When selecting the sampling frame in October 2012, some of the following keywords were used: downtime, availability, trustworthiness, assurance, web, seals, e-commerce, assurance and model. The aim was to determine the number of articles that viewed a website's availability as an assurance measure. The results revealed that 23% of the articles viewed availability as an assurance measure [120][15], while 77% of the articles did not refer to availability as an assurance measure.

## **4.3 EXPERIMENT 2: INVESTIGATING CORRELATION OF PRAHP ASSURANCE ATTRIBUTES**

### **4.3.1 Introduction**

This section demonstrates how important the selected attributes are in providing assurance in cloud-based e-commerce. This is demonstrated through the hypothesis testing that was done for every attribute that was selected for assessment purposes on PRAHP.

### **4.3.2 Experimental setup**

The proposed model consists of the following assurance measures: AL, AI, P, AS and website availability. The term “adaptive” is used to show that the attribute is not fixed, but rather flexible in such a way that it accommodates revised legislation or different legislation, provided it is specific to the e-commerce environment.

The proposed model is aimed at providing useful information for decision-making to a customer concerning the website's trustworthiness.

In order to transact from a website, the proposed model requires the creation of strong online login credentials.

Thereafter, a customer provides input through a short survey, to determine if the customer has read the policies displayed and secondly if the customer has experienced a bad or good shopping encounter through the website in the past or not. The model aggregates the user's input together with the following attributes: policies, legislation, ISO standard and website availability. The model checks the presence of the policies and the last policy review date to determine currency and provide a rating. Furthermore, a check for compliance with ECT legislation will be conducted to produce an overall website rating. Adoption of the ISO standard, specifically the ISO 27001, will be confirmed by the model on the security of online transactions, specifically encryption. An online check to determine if the website is consistently available and has the latest anti-virus software and latest patch is conducted to ensure that it is not vulnerable to online attacks. The model combines all the attribute information using the cooperative rating based on AHP and PR to strengthen the assurance level. A trustworthy site flashes green and an untrustworthy one flashes red. Detailed discussions of the model attributes are presented in sections A to E. One can see that the proposed model has more beneficial enhancements than the existing ones, such as the trusted cloud data security certification and the KYPLEX [121].

In the trans-border cloud environment the application of laws becomes very complex in the event of a privacy or security breach if the applicable laws have not been specified from the onset [122]. In terms of providing e-commerce assurance, laws have been found to be an assurance measure [114]. Different e-commerce laws that are specific can be used with the model. For the purposes of this study, South African legislation will be used because of its specific provisions in terms of e-commerce environments. The ECT Act provisions will be used as measures for aggregation in the e-commerce environment, where the final rating will alert the customer whether the website that is hosted in a cloud environment is safe to transact from or not.

In order to determine the significance of assurance attributes, the following hypotheses were tested:

#### **A. Adaptive legislation as an assurance measure**

A testable null directional correctional hypothesis that is set for this attribute is:

$H_0^1$ : *The level of adaptive legislation of a country is not positively associated with other assurance measures.*

In testing this proposition, explanatory research is required, as shown in **Table 8**.

#### **B. Adaptive ISO security standard as an assurance measure**

The model checks for the security of transactions in an online environment by checking for the encryption of transactions on the website. This check, together with the other attributes, will be assessed and aggregated in order to show the final website assurance rating. A testable null directional correctional hypothesis that is set for this attribute is:

$H_0^2$ : *The level of adaptive ISO standards and other assurance measures is negatively associated.*

In testing this proposition, explanatory research is required, as shown in **Table 8**.

#### **C. Policies as an assurance measure**

Policies in a cloud environment are critical, so that consumers can know and understand how their personal information will be handled in terms of privacy and which laws will apply in the event of a breach. Specifying the laws applicable to policy statements will be an improvement on existing policy models. A testable null directional causal hypothesis that is set for this attribute is:

$H_0^3$ : *The level of policies of a business enterprise does not positively influence other assurance measures.*

In testing this proposition, explanatory research is required, as shown in **Table 8**.

#### **D. Advanced security features as an assurance measure**

Information security in a cloud-based e-commerce environment is crucial in order to gain and maintain online customer trust. CSPs need to provide leading edge security and auditing capabilities to keep up with meeting the customer's assurance needs.

Customers need to feel secure from the login phase to checkout. A testable null directional causal hypothesis that is set for this attribute is:

$H_0^4$  : *The level of strength of advanced user security does not influence other assurance measures.*

In testing this proposition, explanatory research is required, as shown in **Table 8**.

#### **E. Site availability as an assurance measure**

Website availability is crucial in the cloud-based environment. Service disruptions ought to be minimal for customers to gain and maintain trust in an online vendor store. A testable null directional correctional hypothesis that is set for this attribute is:

$H_0^5$  : *The level of e-commerce site availability and other assurance measures is negatively associated.*

In testing this proposition, explanatory research is required, as shown in **Table 8**.

#### **4.3.3 Descriptive and correlation analysis**

**Table 8** contains statistical data, which was produced by conducting a survey of journals from the IEEE and Science Direct databases based on the criteria of whether they were e-commerce transacting sites or not. The survey was conducted to determine if the following attributes had been identified as assurance measures in any of the sampled journals and e-commerce websites: AL, AI, P, A and AS. The sampling frame was October 2012 and the journals were sampled based on their relevance to the topic of this research, where specific keywords were used. The main aim was to determine the number of articles in support of or against the proposed attributes as assurance measures.

**Table 8: Sampled dataset from journal articles and real-life data from e-commerce sites**

Sample no	Sampled Cases	Legislation		ISO		Policies		Security		Availability	
		Y	UND	Y	UND	Y	UND	Y	UND	Y	UND
1	Sample size 8;db1, wrt legislation	63%	37%	0%	100%	63%	37%	100%	0%	0%	100%
2	Sample size 10;db2, wrt legislation	30%	70%	10%	90%	80%	20%	30%	70%	0	100%
3	Sample size 15;db3,wrt legislation	7%	93%	7%	93%	93%	7%	100%	0%	85%	15%
4	Sample size 5;db1, wrt ISO	0%	100%	0%	100%	0%	100%	100%	0%	0%	100%
5	Sample size 10;db2, wrt ISO	0	100%	10%	90%	0%	10%	100%	0%	0%	100%
6	Sample size 10;db3,wrt ISO	20%	80%	10%	90%	100%	0%	100%	0%	0%	100%
7	Sample size 5;db1, wrt Policy	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
8	Sample size 10;db2, wrt Policy	10%	90%	0%	100%	100%	0%	100%	0%	0%	100%
9	Sample size 15;db3,wrt Policy	7%	93%	0%	100%	93%	7%	100%	0%	0%	100%
10	Sample size 5;db1, wrt Security	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
11	Sample size 15;db2, wrt Security	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
12	Sample size 15;db3,wrt Security	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
13	Sample size 10;db1, wrt Availability	0%	100%	0%	100%	90%	10%	90%	10%	50%	50%
14	Sample size 10;db2, wrt Availability	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%
15	Sample size 15;db3,wrt Availability	0%	100%	0%	100%	100%	0%	100%	0%	0%	100%

Keys: db1 = IEEE database, db2 = Science direct database,wrt = with respect to, Y = Yes, UND = Undecided.

The Pearson's correlation coefficient (R) in [123] was implemented and confirmed with Excel Macro to compute the relationships in **Table 8**. Any two attributes were chosen at random to test for possible relationships, as shown below:

*H1: The level of adaptive legislation of a country is not positively associated with other assurance measures.*

**FINDINGS:** The result of the macro implemented implies:

Corr(Legislation: ISO) = 0.2.

**DECISION:** Since the correlation result > 0, Corr (Legislation: ISO) = **0.2**; the above proposition is rejected, which implies that the level of adaptive legislation of a country is positively associated with any other assurance measure.

*H2: The level of adaptive ISO standards and other assurance measures is negatively associated.*

**FINDINGS:** The result of the macro implemented implies: Corr(ISO: Availability) = **0.1769**.

**DECISION:** Since the correlation result > 0, the above proposition is rejected, which implies that the level of adaptive ISO standards and other assurance measures is positively associated.

*H3: The level of policy of a business enterprise does not positively influence other assurance measures.*

**FINDINGS:** The result of the macro implemented implies:  $\text{Corr}(\text{Policies: Availability}) = 0.12$ .

**DECISION:** The correlation result  $> 0$  suggests the rejection of the above proposition. This implies that the level of policy of a business enterprise does positively influence other assurance measures.

*H4: The level of strength of advanced user security does not influence other assurance measures.*

**FINDINGS:** The result of the macro implemented implies:  $\text{Corr}(\text{Security : Availability}) = 0.0353$ .

**DECISION:** The correlation result  $> 0$  suggests the rejection of the above proposition. This suffices to prove that the level of strength of advanced user security does influence other assurance measures. The correlational graph that emerged from these direct or indirect interrelationships is shown in **Figure 25**.



**Figure 25: Emerged correlational graph of the assurance measures**

The results above suggest necessary or supporting conditions to say that the assurance measures could serve as the building blocks of the intelligent model in **Figure 15** and are compliant for accessing the trustworthiness of cloud-based e-commerce sites.



## 4.4 EXPERIMENT 3: PRAHP ASSURANCE FOR SIZEABLE GENERAL E-COMMERCE ENTERPRISES

### 4.4.1. Introduction

This section provides the discussion and details of the experiment that was done on general e-commerce sites using the proposed model, PRAHP, to test the reliability and robustness of the model.

### 4.4.2. Experimental setup: General e-commerce sites

Ten e-commerce websites were selected and they were categorised based on the number of links (inbound, outbound and external links). The real names of the websites that have been assessed have been withheld for confidentiality reasons and they have been replaced by website names A to J. A description of the websites has been added to illustrate the type of e-commerce service offered by a particular website.

**Table 9: E-commerce website descriptions**

Website Name	E-commerce website description	Size of website in terms of links
A	South African IT news website	Small
B	South African online payment	Medium
C	International events reservations	Large
D	South African restaurants, shopping advertisements and specials	Small
E	South African online auctions	Medium
F	Targeted marketing services through social media	Medium
G	One of the biggest networking sites, which sells advertising packages for businesses	Large
H	South African e-commerce site, which sells a diverse range of commodities and services	Medium
I	Events online booking platform	Small
J	International e-commerce website that sells a variety of commodities	Large

A selection of key attributes was made based on the importance of these attributes in terms of the literature and also as evidenced by the use of these attributes by some of the websites reviewed for the purposes of this study. The e-commerce assurance attributes were introduced in chapters 3 and 4. An assessment of the website attributes was conducted using the macro-based AHP assessment tool [96], which allowed for the capturing of the attributes and the assignment of weights using the scale shown in **Figure 18**.

#### 4.4.3. PRAHP assurance for small and large general-commerce enterprises

##### (1) AHP: Pairwise comparison matrix level-1 with respect to the goal

The aim of this section is to demonstrate how each of the attributes in website A was assessed using the tool with reference to the goal.

As depicted in **Table 10**, the attributes are assessed through the comparison of a pair of attributes such as policy and legislation, using the scale in **Figure 18**. A weighting is assigned based on the degree of importance of an attribute, e.g. a comparison between policy and ISO favoured policy according to **Table 10**.

**Table 10: Pairwise comparison and AHP-1 with respect to the goal**

	<b>L</b>	<b>P</b>	<b>AS</b>	<b>A</b>	<b>ISO</b>	AHP-1 with respect to the goal	
<b>L</b>	1	1	1/2	1	1	0.174	17.4%
<b>P</b>	1	1	1	2	2	0.256	25.6%
<b>AS</b>	2	1	1	2	2	0.285	28.5%
<b>A</b>	1	1/2	1/2	1	1	0.142	14.2%
<b>ISO</b>	1	1/2	1/2	1	1	0.142	14.2%

**Table 11: Last iteration for convergence and AHP-4 with respect to the goal**

	<b>L</b>	<b>P</b>	<b>AS</b>	<b>A</b>	<b>ISO</b>	AHP-4 with respect to the goal	
<b>L</b>	0.174418619	0.174418607	0.174418599	0.174418599	0.174418599	0.17	17.40%
<b>P</b>	0.255813942	0.255813967	0.255813951	0.255813951	0.255813951	0.26	25.60%
<b>AS</b>	0.284883719	0.284883713	0.284883725	0.284883725	0.284883725	0.29	28.50%
<b>A</b>	0.14244186	0.142441856	0.142441863	0.142441863	0.142441863	0.14	14.20%
<b>ISO</b>	0.14244186	0.142441856	0.142441863	0.142441863	0.142441863	0.14	14.20%

$$CI=0.01526 \quad \lambda=5.061046513$$

Half the matrix was populated diagonally where the rest of the cells were automatically calculated. Normalisation as inverse is done through the automated iteration process, which results in the convergence of the last iteration in **Table 11**. According to the percentage allocation, the advanced security attribute has the highest assurance rating, as shown in **Tables 10** and **11**. The normalisation is done through the automated iteration process, which results in the formation of the last iteration in **Table 11**, showing the final result of the

normalised matrix with the  $\lambda$  and the consistency index. One can see that the results are valid with  $CI=0.01526$ , which is less than 1%, stated in step 6 of paradigm 1.

*(2) AHP: Pairwise comparison matrix level 2 with respect to level- 1*

The aim of the level 2 comparison matrix is to assess the level of importance of each assurance indicator (RAG) with respect to level 1 attributes. In this case the policy attribute for website A was assessed by using the RAG indicators to determine the level of importance. Each indicator was assigned a weighting based on **Figure 18**, e.g. 1/7 based on the level 1 importance, and this was automatically calculated by the automated macro tool. **Table 12** shows the initial assessment of RAG indicators based on a level 1 attribute, i.e. P. Half the matrix was diagonally populated and the rest of the cells were automatically calculated by the tool. The sum of these status percentages added up to 100% and this constituted the level 2 vectors.

**Table 12: Pairwise comparison and AHP-1 with respect to level 1**

	<b>R</b>	<b>A</b>	<b>G</b>	<b>AHP-1 with respect to level 1</b>	
<b>R</b>	1	1/2	1/3	0.174	17.4%
<b>A</b>	2	1	1/3	0.228	22.8%
<b>G</b>	3	3	1	0.598	59.8%

**Table 13: Last iteration for convergence**

	<b>R</b>	<b>A</b>	<b>G</b>	<b>AHP-4 with respect to level 1 (policy)</b>	
<b>R</b>	0.173913055	0.173913037	0.173913	0.174	17.4%
<b>A</b>	0.228260873	0.22826088	0.228261	0.228	22.8%
<b>G</b>	0.597826073	0.597826073	0.597826	0.598	59.8%

$$\lambda=3.067029 \quad CI=0.03351$$

*(3) Composite vectors*

The results of attribute assessment on levels 1 and 2 were combined to come up with composite vectors, which are the AHP overall website rating.

This is illustrated in step 8 of paradigm 3. Equations 4, 5 and 6 were used for composite vector calculation.

**Table 14: Composite matrix percentage for website A**

<b>R</b>	20.0%
<b>A</b>	30.0%
<b>G</b>	50.0%

Based on the composite vector equations, the results of the RAG status show the percentage allocation as shown in **Table 14**. From the AHP results only one can see that website A is safer to transact on, since green has the highest percentage indicator, but the final PRAHP assurance rating is complemented with evidential assessment of PR.

#### *(4) Page ranking*

An initial matrix of websites A to J was developed in **Table 15**. Where a website connected to another website in terms of the outbound and inbound links, a value of 1 was assigned and where no links were present a value of 0 was captured, as shown in step 1 of PR side paradigm 3. The last column of the matrix of **Table 16** contains the sum total, SUM (A+...+J), of the values in a particular row, as shown in steps 2 and 3 of paradigm 3. The last row, C<sub>J</sub>, consists of the sum total SUM = (A+...+J) of all the values in a specific column.

**Table 15: Initial Page rank matrix**

<b>Lij</b>	<b>A</b>	<b>B</b>	<b>C</b>	<b>D</b>	<b>E</b>	<b>F</b>	<b>G</b>	<b>H</b>	<b>I</b>	<b>J</b>	<b>Total</b>
<b>A</b>	1	0	0	0	0	1	0	0	1	1	4
<b>B</b>	0	1	0	0	0	0	0	0	1	1	3
<b>C</b>	0	0	1	0	0	0	0	0	1	1	3
<b>D</b>	0	0	0	1	0	0	0	0	1	1	3
<b>E</b>	0	0	0	0	1	0	0	0	1	1	3
<b>F</b>	1	0	0	0	0	1	0	0	1	1	4
<b>G</b>	0	0	0	0	0	0	1	0	1	0	2
<b>H</b>	0	0	0	0	0	0	0	1	1	1	3
<b>I</b>	1	1	1	1	1	1	1	1	1	1	10
<b>J</b>	1	1	1	1	1	1	0	1	1	1	9
<b>CJ</b>	4	3	3	3	3	4	2	3	10	9	44

**Table 16: Final Page rank matrix**

Lij	A	B	C	D	E	F	G	H	I	J	Sum product	Pi
A	0.25	0.00	0.00	0.00	0.00	0.25	0.00	0.00	0.10	0.11	0.98	0.98
B	0.00	0.33	0.00	0.00	0.00	0.00	0.00	0.00	0.10	0.11	0.74	0.78
C	0.00	0.00	0.33	0.00	0.00	0.00	0.00	0.00	0.10	0.11	0.74	0.78
D	0.00	0.00	0.00	0.33	0.00	0.00	0.00	0.00	0.10	0.11	0.74	0.78
E	0.00	0.00	0.00	0.00	0.33	0.00	0.00	0.00	0.10	0.11	0.74	0.78
F	0.25	0.00	0.00	0.00	0.00	0.25	0.00	0.00	0.10	0.11	0.98	0.98
G	0.00	0.00	0.00	0.00	0.00	0.00	0.50	0.00	0.10	0.00	0.56	0.63
H	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.33	0.10	0.11	0.74	0.78
I	0.25	0.33	0.33	0.33	0.33	0.25	0.50	0.33	0.10	0.11	2.61	2.37
J	0.25	0.33	0.33	0.33	0.33	0.25	0.00	0.33	0.10	0.11	2.30	2.11
PJ	1.0	0.8	0.8	0.8	0.8	1.0	0.6	0.8	2.4	2.1		
Pi	1.0	0.8	0.8	0.8	0.8	1.0	0.6	0.8	2.4	2.1		

Following the matrix in **Table 15**, other matrices were created for iterative processes and the final results of the iteration are shown in **Table 16**, which shows convergence on the last two rows. In other words, convergence was reached after repeating step 8 of paradigm 3.

According to the information in **Table 16**, an additional row was created, called  $P_J$ ; this row contained the figures from the previous table row,  $C_J$ .

The aim of the creation of row  $P_J$  was to generate normalisation values for all the rows and columns where the values in a cell were divided by the corresponding values in cell  $P_J$ . The values would be placed in particular cells, e.g. the value on the first cell,  $L_{ij}/4=0.25$ . The value of 0.25 would then be captured on cell  $L_{ij}$ . The sum product column was also created, which consisted of sum row values as illustrated in step 5 of paradigm 3. The sum product was computed for each row. The algorithm is also illustrated by step 7 of paradigm 3.

Further iterations were done by simply taking the values on the  $P_i$  column and replacing the previous table's  $P_J$  values. The iteration was done until convergence of the  $P_J$  values and  $P_i$  values, as shown in **Table 16**.

#### (5) Consensus decision

The results of the AHP and PR assessments have been presented in **Table 17**, where different combinations yielded different results using equation 7. Status results are presented using the following status findings: T = trustworthy, PT = partially trustworthy and UT = untrustworthy.

Based on decision concepts of the decision table, **Table 17** validates the results of the 10 websites using the proposed PRAHP framework with customers' open assessments. The last column shows the comments by customers regarding their dissatisfaction with some aspect of the e-commerce website.

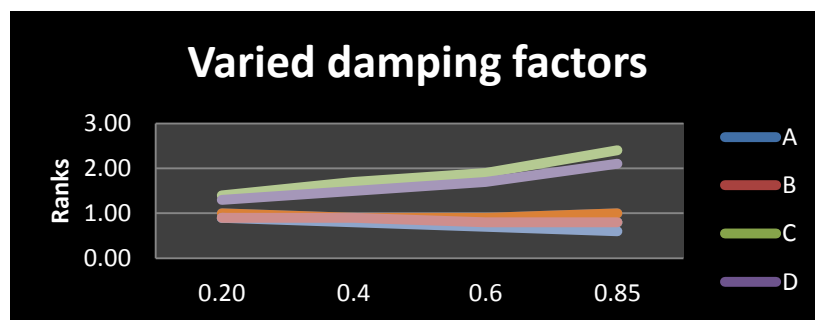
**Table 17: Validation results**

Website labels	Results	Validation comments
A	AHP(Green)+PR(Green) =Trustworthy	No comment = trustworthy
B	AHP(Green)+PR(Red) = Partially Trustworthy	No comment = partially trustworthy
C	AHP(Amber)+PR(Red) = Untrustworthy	“My husband has died some months ago but I have just discovered that someone has been transacting on his account through your website, how is that possible?”
D	AHP(Green)+PR(Green) = Trustworthy	No comment = trustworthy
E	AHP(Red)+PR(Green) = Partially Trustworthy	No comment = partially trustworthy
F	AHP(Amber)+PR(Amber) = Partially Trustworthy	No comment = partially trustworthy
G	AHP(Red)+PR(Red) = Untrustworthy	“I just got informed that someone logged into my account from a strange location, how can I stop this?”
H	AHP(Amber)+PR(Red) = Untrustworthy	“My account for this website has been hacked and my email taken over, please help.”
I	AHP(Green)+PR(Green) =Trustworthy	No comment = trustworthy
J	AHP(Amber)+PR(Green) = Partially Trustworthy	No comment = partially trustworthy

#### 4.4.4. Effects of varied damping factor $d$ on PRAHP

Most PR-based applications use the damping factor  $d$  as a primary factor in defining rating activities. This is attributed to the fact that most rating applications are robust or sensitive to  $d$ , as this affects the quality of the rating. Therefore, the degree of PR propagation in PRAHP from one page to another by a link is primarily determined by the value of  $d$  and it is often iterated between 0 and 1.

The objective here is to verify a hypothesis that the higher the value of  $d$ , the larger the effect of inbound links and the more evenly distributed the ratings over the other pages of a site are. By varying  $d$ , the robustness of PRAHP is also tested evenly at  $d = 0.2$ ,  $0.4$ , and  $0.6$  in addition to the results at  $d = 0.85$ . This trend is shown in **Figure 26**.

**Figure 26: Varied damping factors**

One can see that the PRAHP model offers a more realistic assessment of website trustworthiness based on the PR technique combined with the AHP. **Figure 26** illustrates that as the damping factor increases, the website rank's propagation tends to be distributed.

#### **4.5 EXPERIMENT 4: PRAHP EVALUATION ON PRIVATE AND PUBLIC CLOUD-BASED ASSURANCE**

##### **4.5.1 Introduction**

This section details the experiment that was done using PRAHP on cloud-based e-commerce environments.

##### **4.5.2 Experimental setup on cloud-based sites**

As introduced in section 4.1, 10 cloud-based e-commerce sites were used for the PRAHP experiments. These websites are live sites belonging to different e-commerce stores, which are hosted in the cloud. Some of the websites were hosted on the private cloud, which is an isolated infrastructure hosted in the cloud. The public cloud is the cloud infrastructure meant for public use and it is shared among users. The details of the experiments of PRAHP's evaluations are explained in the next section.

##### **4.5.3 Assurance of private and public e-commerce cloud sites**

The criteria for website selection included the number of inbound/outbound links, self-links and the type of cloud model, namely whether it is a public or private cloud. The website links have been classified as high, medium and low.

Pseudo-names of websites A to J were used and a description of the websites was added to illustrate the type of services offered by a particular website, as shown in **Table 18**.

**Table 18: Cloud website descriptions**

Website name	Private and Public Cloud Website Description	Size	Cloud deployment Model
A	Events and online booking system	Small	Private
B	Marketing services via online media	Medium	Public
C	E-commerce exchange	Medium	Private
D	Online payment service providers	Small	Private
E	Technology news broadcaster	Small	Private
F	Arts events management system	Small	Private
G	Online marketing and shopping directory	Large	Private
H	Online payment platform	Medium	Private
I	E-commerce social network with advertising capabilities	Large	Public
J	E-commerce social network with advertising capabilities	Large	public

The literature survey and the assessment of challenges faced by cloud websites guided the selection of attributes deemed important in the cloud. The attributes used in this experiment were AL, AI, A, AS and P. The attributes were assessed based on the tool depicted in **Figure 18**.

**(a) AHP: Pairwise comparison matrix level 1 with respect to the goal**

This section demonstrates attribute assessment using the macro-based AHP tool referred to in section 4.1. A paired comparison of attributes is used to determine the importance of a particular attribute on a website. A weighting is objectively assigned based on the degree of importance of every attribute, e.g. in a comparison between AI and AL on website A, AI is less important according to **Table 19**.

The initial pairwise comparison is shown in **Table 19** for all the attributes, where all the attributes are compared with all others.

**Table 19: Initial pairwise comparison and AHP-level 1**

	AL	P	AS	A	AI	AHP-1
AL	1	1	1	1	3	23.90%
P	1	1	1	1	2	21.90%
AS	1	1	1	1	2	21.90%
A	1	1	1	1	2	21.90%
AI	1/3	1/2	1/2	1/2	1	10.20%



**Table 20: Final iteration for convergence and AHP-level 4**

	AL	P	AS	A	AI	AHP-4
AL	0.232	0.232142857	0.232142857	0.232142857	0.232142857	23.20%
P	0.222	0.221938776	0.221938776	0.221938776	0.221938775	22.20%
AS	0.222	0.221938776	0.221938776	0.221938776	0.221938775	22.20%
A	0.222	0.221938776	0.221938776	0.221938776	0.221938775	22.20%
AI	0.102	0.102040816	0.102040816	0.102040816	0.102040816	10.20%

$$\lambda = 5.022534014$$

$$CI = 0.000563$$

**Table 20** shows the results of the final pairwise comparison. Half the matrix was populated on the tool diagonally, whereas the rest of the cells were automatically populated. Normaliation was performed through the automated iteration process, which resulted in the formation of the last iteration in **Table 20**, showing the final result of the normalised matrix with  $\lambda \approx 5 \Rightarrow$  five attributes. One can see that the results are valid with  $CI = 0.000563$ , which is less than 1% stated in step 6 of paradigm 1, section 3.5.2.1.

#### (b) AHP: Pairwise comparison matrix level 2 with respect to level 1

The aim of the level 2 comparison matrix is to assess the level of importance of each assurance indicator (RAG) with respect to level 1 attributes, as illustrated in paradigm 2, step 1. In this case the availability attribute for website A was assessed by using the RAG indicators to determine the level of importance. Each indicator was assigned a weighting based on the scale shown in **Figure 18**.

**Table 21** shows the initial assessment of RAG indicators based on the level 1 attribute, i.e. availability. Half the matrix was diagonally populated and the rest of the cells were automatically calculated by the tool. The sum of these status percentages added to up 100% and this constituted the level 2 vectors in **Table 22**;  $\lambda \approx 3 \Rightarrow$  three attributes. **Table 23** shows the final results with respect to all the attributes. Based on these results, one can see that the results are acceptable, as they are all consistent.

**Table 21: Initial matrix and AHP-level 1 with respect to availability**

	R	A	G	AHP-1	
R	1	1/2	2	0.312	31.20%
A	2	1	2	0.490	49.00%
G	1/2	1/2	1	0.198	19.80%

**Table 22: Final iteration for convergence and AHP level 4 with respect to availability**

	R	A	G	AHP-4	
R	0.291666693	0.291666649	0.291666673	0.292	29.2%
A	0.499999992	0.500000019	0.4999999965	0.500	50.0%
G	0.283333315	0.208333332	0.208333362	0.208	20.8%

$$\lambda = 3.062500016 \quad CI = 0.03125$$

**Table 23: Converged results with respect to all the variables**

W.R.T	RAG (Vector %)			Lamda	CI	Acceptability
	R	A	G			
L	16.8%	54.5%	28.7%	3.011494253	0.00575	Consistent
P	20.8%	29.2%	50.0%	3.062500016	0.03125	Consistent
AS	17.4%	22.8%	59.8%	3.067029	0.03351	Consistent
A	29.2%	50.0%	20.8%	3.062500016	0.03125	Consistent
ISO	20.8%	29.2%	50.0%	3.062500016	0.03125	Consistent

### (c) Composite vectors

A combination of the AHP level 1 and 2 assessments from **Table 21** and **Table 22** produced the final AHP website ratings as depicted in **Table 24** as composite vectors. The composite vector equations (4), (5) and (6) were used to generate the ratings, e.g in website A, Red=(23.20\*16.8)+(22.20\*29.2)+.....=40%.

**Table 24: Composite vector matrix percentage for all websites**

Website	RAG (Composite vector %)			Dominant AHP rating
	R	A	G	
A	40%	30.0%	30.0%	Red
B	27%	30.0%	40.0%	Green
C	19%	44.0%	37.0%	Amber
D	21%	38.0%	41.0%	Green
E	15%	60.0%	25.0%	Amber
F	50%	30.0%	20.0%	Red
G	15%	30.0%	55.0%	Green
H	16%	60.0%	24.0%	Amber
I	24%	30.0%	46.0%	Green
J	22%	30.0%	48.0%	Green

**Table 22** shows the final AHP results based on the RAG ratings, which were linked to the percentage allocation rating per website. From the results one can see that websites A and F are unsafe to transact from, whereas websites C, E and H should be used with caution. Only websites B, D, G, I and J are safe to transact from.

#### **(d) Evidential reasoning with Page ranking**

In order to leverage on the AHP ratings and to increase the PRAHP assurance of the cloud sites reliability, the matrix of websites from website A to J was developed, as shown in **Table 25**. Where a website is connected with another website in terms of outbound and inbound links, a value of 1 was assigned, and where no links were present, a value of 0 was captured, as shown in step 1 of PR in paradigm 3, section 3.5.2.4.

The last column of the matrix contains the sum total SUM ( $A+...J$ ) of the values in a particular row, as shown in steps 2 and 3 of paradigm 3. The last row,  $C_j$ , consists of the sum total SUM= ( $A+...J$ ) of all the values in a specific column.

Table 25: Initial Page rank matrix

$L_{iJ}$	A	B	C	D	E	F	G	H	I	J	Sum Total
A	1	0	0	0	0	0	0	0	0	0	1
B	0	1	0	0	0	0	0	0	0	1	2
C	0	0	1	0	0	0	0	0	0	1	2
D	0	0	0	1	0	0	0	0	0	1	2
E	0	0	0	0	1	0	0	0	0	0	1
F	0	0	0	0	0	1	0	0	1	0	2
G	0	0	0	0	0	0	1	0	1	0	2
H	0	0	0	0	0	0	0	1	1	1	3
I	0	0	0	0	0	1	1	1	1	1	5
J	0	1	1	1	0	0	0	1	1	1	6
$C_J$	1	2	2	2	1	2	2	3	5	6	

Table 26: Final Page rank matrix converged at 17<sup>th</sup> iteration

$L_{iJ}$	A	B	C	D	E	F	G	H	I	J	Sum prod	$P_i$	Rank	Indicators
A	1	0	0	0	0	0	0	0	0	0	1.0	1	3	PI
B	0	0.5	0	0	0	0	0	0	0	0.2	0.8	0.8	4	PI
C	0	0	0.5	0	0	0	0	0	0	0.2	0.8	0.8	4	PI
D	0	0	0	0.5	0	0	0	0	0	0.2	0.8	0.8	4	PI
E	0	0	0	0	1	0	0	0	0	0	1.0	1	3	PI
F	0	0	0	0	0	0.5	0	0	0.2	0	0.7	0.7	5	LI
G	0	0	0	0	0	0	0.5	0	0.2	0	0.7	0.7	5	LI
H	0	0	0	0	0	0	0	0.3	0.2	0.2	1.0	1	3	PI
I	0	0	0	0	0	0.5	0.5	0.3	0.2	0.2	1.7	1.6	2	I
J	0	0.5	0.5	0.5	0	0	0.0	0.3	0.2	0.2	2.2	2	1	I
$P_i$	1	0.8	0.8	0.8	1	0.7	0.7	1	1.6	2		10.4		

Other matrices were created from the initial matrix for iterative processes and the final results of the iteration are shown in **Table 26**, which shows convergence on the last row  $P_i$  and column  $P_i$ . In other words, the ranking appears valid, since  $\sum P_i \approx 10 \Rightarrow 10$  sites. The rank column in **Table 26** shows the relevance or quality of a website. The sum product column was also created, which consisted of the sum row values as illustrated in step 5 of paradigm 3. The sum product was computed for each row.

In order to conform with the three indicators of AHP,  $P_i$  is ranked and categorised into three indicators as important = I, partially important = PI and less important = LI (see step 9, paradigm 3). Hence PR ratings are shown in **Table 27**.

Websites J and I seem to be more popular and have a good reputation, since their ratings are better than those of websites F and G. This could imply that J and I have inbound links from secured and repeated sites such as the Microsoft website.











**Table 27: Cloud websites ordered, ranked and rated according to importance**

	J	I	H	E	A	D	C	B	F	G
Pi	2	1.6	1	1	1	0.8	0.8	0.8	0.7	0.7
Rank	1	2	3	3	3	4	4	4	5	5
Ratings	I	I	PI	PI	PI	PI	PI	PI	LI	LI

#### 4.2.2.5 Consensus decision and consumer validation comments

**Table 28** shows the overall ratings and reliability website ratings based on the PRAHP assessments, using equation 7. The last column of the table shows comments posted on some of the unsecured websites by dissatisfied customers, which validate the PRAHP consensus rating results that were obtained.

**Table 28: Final PRAHP website ratings**

Website labels	PRAHP Results	Validation comments
A	AHP(Red)+PR(PI)=>Untrustworthy 	"There was a duplicate charge on my account, please close my account and refund as I never bought anything from your website"
B	AHP(Green)+PR(PI)=>Partially Trustworthy 	No comment=Partially Trustworthy
C	AHP(Amber)+PR(PI)=>Partially Trustworthy 	No comment=Partially Trustworthy
D	AHP(Green)+PR(PI)=>Partially trustworthy 	No comment= Partially Trustworthy
E	AHP(Amber)+PR(PI)=>Partially trustworthy 	No comment= Partially Trustworthy
F	AHP(Red)+PR(LI) =>Untrustworthy 	"the some of the information we stored on your cloud has been unavailable for days, please confirm when it will be available"
G	AHP(Green)+PR(LI)=>Partially Trustworthy 	No comment=Partially Trustworthy
H	AHP(Amber)+PR(PI)=>Partially Trustworthy 	No comment=Partially Trustworthy
I	AHP(Green)+PR(I) =>Trustworthy 	No comment=Trustworthy
J	AHP(Green)+PR(I) =>Trustworthy 	No comment =Trustworthy

The status results in **Table 28** are accurate and based on these results it is evident that websites A and F, which have a red rating and a PI for PR and red AHP and an LI for PR respectively, are classified as untrustworthy for transacting purposes. On the other hand, I and J are far more trustworthy sites, based on PRAHP. These results provide a comprehensive view of the website rating.

#### 4.5.4 Effects of varied inbound links on PRAHP and second validation

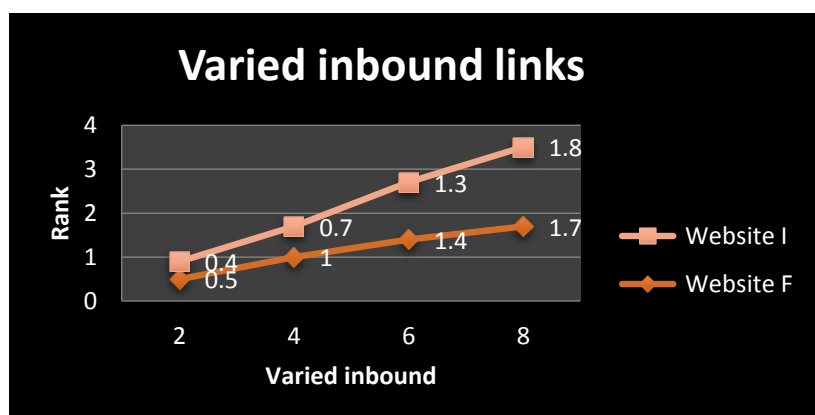
The effects of inbound links on PRAHP, especially its reliability, were checked in this experiment. The results are depicted in **Figure 27**.

The inbound and outbound links are used by many PR-based applications as a primary measure for a website rating mechanism. This is attributed to the fact that most website rating applications are sensitive to the number of links, as this affects the status of the rating. Therefore the degree of PR propagation in PRAHP from one page to another by a link is primarily determined by the number of links. The PR is often iterated between 0 and 1.

The objective here is to verify a hypothesis of the varied inbound links and their impact using the null ( $H_0$ ) and alternative ( $H_1$ ) hypothesis.

**$H_0$ :** Increase in inbound links for a web page does not increase that page's PR.

**$H_1$ :** Increase in inbound links for a web page increases that page's PR.



**Figure 27: Varied inbound links for website I and F**

**Figure 27** shows the new Pi values of the private website F and public website I as responses to the adjustment of varied inbound links.

From the results, it is clear that as the number of links increase, both website ranks increase, which suggests to the author that  $H_0$  is rejected, and  $H_1$  is accepted.

#### 4.6 EXPERIMENT 5: PRAHP evaluation on B2C and B2B e-commerce websites

The reliability and robustness of PRAHP was tested through the experiments that were conducted in real B2C and B2B e-commerce websites. This section provides the details on how the experiments were conducted. As in section 4.5, the same attributes that were used for the cloud-based e-commerce websites were used in this experiment also.

##### 4.6.1 Experimental setup

Ten carefully selected e-commerce websites listed and described in **Table 29** were assessed for the purposes of this study. The sites selected for the PRAHP experiments were a combination of B2B and B2C websites. These websites were chosen based on the following criteria: e-commerce deployment model and the number of links, e.g. self-links/inbound links per website. The names of the websites have been withheld for confidentiality reasons; instead alphabetic designations are used from websites GH to YZ. The website descriptions have been added to bring context to the discussion.

**Table 29: Website descriptions**

Website name	E-commerce type	E-commerce website description	Website size based on links
GH	B2C	News and IT equipment e-tailer	Small
IJ	B2B	Online payment platforms for e-tailers	Medium
KL	B2C	Online events and reservations booking platform	Large
MN	B2C	Dining advertising platform	Small
OP	B2B	E-auctions platform	Medium
QR	B2C	Targeted marketing services through social media	Medium
ST	B2C	Networking and advertising platform	Large
UV	B2C	E-tailer offering a wide range of commodities	Medium
WX	B2C	Ticket selling platform for events	Small
YZ	B2B	E-commerce website offering a diverse list of commodities	Large

An AHP assessment tool (macro-based), was used to weigh the assessments [98]. The tool was developed on the Microsoft Excel platform coded with AHP mathematical equations for the assessment of the selected attributes. The tool required the number of criteria to be specified and in this instance five criteria were captured for the five attributes. The pairwise comparison matrix was constructed for the five attributes and the weights were assigned using the scale in **Figure 18**.

Real data from customer input was used to enhance and support the results by supplying a qualitative and quantitative measure of that information. The ratings were automatically converted into percentage form, which totalled 100%. These AHP assessment results constituted level 1 vectors (refer to **Table 30**).

#### 4.6.2 Construction of AHP pairwise comparison matrix

##### (a) Pairwise comparison matrix level 1 with respect to the goal

**Table 30** shows the initial step in AHP for conducting a pairwise comparison of the attributes with regard to the goal. All attributes are compared to determine which attribute has a stronger trustworthiness weighting.

The upper triangular matrix is populated diagonally based on the AHP software and the lower triangular cells are automatically populated from the principles.

Based on the results displayed in **Table 30**, the results of the initial comparison matrix reveal that the AL attribute has the strongest trustworthiness score in a website compared to the rest.

**Table 30: Initial pairwise comparison and AHP-Level 1**

	AL	P	AS	A	AI	AHP 1	
AL	1	3	2	3	3	0.385	39%
P	1/3	1	1/2	2	2	0.165	17%
AS	1/2	2	1	2	2	0.229	23%
A	1/3	1/2	1/2	1	1/2	0.095	10%
AI	1/3	1/2	1/2	2	1	0.127	13%



**Table 31: Final iteration for convergence and AHP-Level 4**

	AL	P	AS	A	AI	AHP- 4	
AL	0.39766527	0.398	0.3977	0.397665	0.397665	0.398	39.8%
P	0.14958154	0.149	0.1496	0.149582	0.149582	0.150	15.0%
AS	0.22214405	0.222	0.2221	0.222144	0.222144	0.222	22.2%
A	0.10633275	0.106	0.1063	0.106333	0.106333	0.106	10.6%
AI	0.12427639	0.124	0.1243	0.124276	0.124276	0.124	12.4%

$$\lambda = 5.169987292 \quad CI = 0.04247$$

The final **Table 31** was obtained after the fourth iteration where AL appears more precise. Since  $\lambda = 5.16$ , which is approximately equal to the number of five attributes that have been assessed, and  $CI = 0.04247$  is less than 0.1, one can see that the results are consistent, as shown in step 6, paradigm 1.

#### **(b) AHP: Pairwise comparison matrix level 2 with respect to level 1**

This assessment entails taking the level 2 assurance indicators and conducting a pairwise comparison of each indicator in relation to the level 1 assurance attribute. i.e. policy in this case.

The level of importance of each assurance indicator (RAG) is assessed by level 2 of the comparison matrix with respect to level 1 attributes. The policy attribute for website GH was assessed using the assessment indicators, i.e. RAG, in order to determine their importance levels. The scale depicted in **Figure 18** through the AHP tool was used to assign weights based on RAG. The initial assessment of RAG based on the level 1 attribute, i.e. policy, is shown in **Table 32**. The matrix was populated diagonally where the remaining cells were populated automatically by the AHP macro-based tool.

**Table 32** shows the results of the initial pairwise comparison of level 2 indicators with respect to policy in level 1, where it is evident that green is a dominating indicator at 49% and red is recessive. **Table 33** shows the final iteration of level 2 vectors where the sum of these status percentages totals 100%.

**Table 32: Initial matrix and AHP level 1 with respect to policy**

	R	A	G	AHP-1	
R	1	1/2	1/2	0.198	19.80%
A	2	1	1/2	0.312	31.20%
G	2	2	1	0.49	49.00%

**Table 33: Final iteration for convergence and AHP level 2 with respect to policy**

	R	A	G	AHP-4	
R	0.2083334	0.208333315	0.208333332	0.208	20.80%
A	0.2916667	0.291666693	0.291666649	0.292	29.20%
G	0.5	0.49999992	0.500000019	0.5	50.00%

$$\lambda = 3.062500016 \quad CI = 0.03125$$

Based on these results,  $\lambda = 3.062500016 \approx 3$  attributes,  $CI = 0.03125 < 0.1$ , it is clear that the results are all consistent and acceptable, as shown in step 6, paradigm 1. The final level 2 and level 1 AHP results of website GH using all the attributes are shown in **Table 34**.

**Table 34: Converged results with respect to all the variables for website GH**

	RAG (Vector %)					
W.R.T	R	A	G	Lamda ( $\lambda$ )	CI	Acceptability
AL	20.80%	29.20%	50.00%	3.0625	0.01325	Consistent
P	20.80%	29.20%	50.00%	3.0625	0.01325	Consistent
AS	16.50%	22.90%	60.60%	3.067029	0.03351	Consistent
A	17.00%	23.00%	60.00%	3.067029	0.03351	Consistent
AI	21.00%	29.00%	50.00%	3.0625	0.01325	Consistent

### (c) Composite vectors

In this section, the implementation results of level 1 and 2 assessments are integrated for all websites and presented in **Table 35**. For every website, a dominating AHP rating is reflected in the last column of **Table 35**. The combined AHP level 1 and 2 assessments yield the final AHP site ratings, using composite vectors, which are shown in **Table 35**.

For example, a final rating for website MN was generated using equations (4), (5) and (6), i.e. a dominating status *green* is computed as:

$$\text{Green} = (39.8 \times 50) + (10.6 \times 60) + \dots = 40\%$$

**Table 35: Composite vector matrix from implementation of all websites**

Website	RAG Composite Vector (%)			Dominant AHP rating
	R	A	G	
GH	15.00%	59.50%	25.50%	Amber
IJ	45.00%	35.00%	20.00%	Red
KL	34.80%	40.00%	25.20%	Amber
MN	33.90%	26.10%	40.00%	Green
OP	50.70%	29.20%	20.10%	Red
QR	19.00%	44.00%	37.00%	Amber
ST	15.20%	59.40%	25.40%	Amber
UV	25.00%	45.00%	30.00%	Amber
WX	19.80%	50.10%	30.10%	Amber
YZ	23.30%	30.60%	46.10%	Green

The final AHP results based on RAG are depicted as percentages in **Table 35**, which add up to 100% for each site. Based on the results, it is evident that the unsafe websites are OP and IJ. The websites that should be used with caution are GH, KL, QR, ST, UV, WX and websites MN and YZ are safe to transact from. However, evidential reasoning of the PRAHP model is essential to give final trustworthiness assurance on the sites with confidence.

#### **(d) Evidential reasoning with page ranking**

In order to supplement the AHP results, the PR technique is introduced through a matrix of website links. **Table 36** depicts the initial PR matrix, which is made up of 10 e-commerce websites that connect to one another through inbound and outbound links.

Where there is a link between sites, a value of 1 is captured in the box and the absence of a link is denoted by 0.

Table 36 shows the initial PR matrix and after 21 iterations the result of the final matrix is shown in **Table 37**. The results in **Table 37** have been ranked based on a scale of 1 to 6, with 1-2 being equated to ‘important’, 3-4 to ‘partially important’ and lastly 5-6 to ‘least important’.

**Table 36: Initial Page rank matrix**

L <sub>ij</sub>	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	Sum Total
GH	1	0	0	0	0	1	0	0	1	1	4
IJ	0	1	0	0	0	0	0	0	1	1	3
KL	0	0	1	0	0	0	0	0	1	1	3
MN	0	0	0	1	0	0	0	0	1	1	3
OP	0	0	0	0	1	0	0	0	1	1	3
QR	1	0	0	0	0	1	0	0	1	1	4
ST	0	0	0	0	0	0	1	0	1	0	2
UV	0	0	0	0	0	0	0	1	1	1	3
WX	0	0	0	0	1	1	1	1	1	1	6
YZ	1	1	1	1	1	1	0	1	1	1	9
C <sub>j</sub>	3	2	2	2	3	4	2	3	10	9	40

Convergence was reached after the iterative process on the initial matrix, which gave the final result shown in **Table 37** as confirmed in column P<sub>i</sub> and row P<sub>i</sub>. The rank column in **Table 37** shows the level of relevance of the websites, with valid ranking, evident from  $\sum P_i = 9.9 \approx 10$  sites.

**Table 37: Final Page rank matrix converged at the 21<sup>st</sup> iteration**

L <sub>ij</sub>	GH	IJ	KL	MN	OP	QR	ST	UV	WX	YZ	Sumprod	P <sub>i</sub>	Rank	Indicator
GH	0.3	0	0	0	0	0.3	0	0	0.1	0.1	1	1	3	PI
IJ	0	0.5	0	0	0	0	0	0	0.1	0.1	0.8	0.8	4	PI
KL	0	0	0.5	0	0	0	0	0	0.1	0.1	0.8	0.8	4	PI
MN	0	0	0	0.5	0	0	0	0	0.1	0.1	0.8	0.8	4	PI
OP	0	0	0	0	0.3	0	0	0	0.1	0.1	0.6	0.7	5	LI
QR	0.3	0	0	0	0	0.3	0	0	0.1	0.1	1	1	3	PI
ST	0	0	0	0	0	0	0.5	0	0.1	0	0.4	0.5	6	LI
UV	0	0	0	0	0	0	0	0.3	0.1	0.1	0.6	0.7	5	LI
WX	0	0	0	0	0.3	0.3	0.5	0.3	0.1	0.1	1.3	1.3	2	I
YZ	0.3	0.5	0.5	0.5	0.3	0.3	0	0.3	0.1	0.1	2.6	2.4	1	I
P <sub>i</sub>	1	0.8	0.8	0.8	0.7	1	0.5	0.7	1.3	2.4		9.9		

The sum product was computed for each row. Three indicators, i.e. important = I, partially important = PI and less important = LI, were used for the P<sub>i</sub> rank in order to align with the AHP indicators (green, amber and red) respectively.

Hence PR ratings are shown in **Table 38**. The most positively ranked websites seem to be YZ and WX, compared to websites UV, OP and ST. This could be attributed to the good security features and the number of links of websites YZ and WX.

The findings in **Table 38** give useful information on the trustworthiness of a particular e-commerce website based on the final PR rating.

**Table 38: B2B and B2C websites ordered, ranked and rated according to importance**

	<b>YZ</b>	<b>WX</b>	<b>GH</b>	<b>QR</b>	<b>IJ</b>	<b>KL</b>	<b>MN</b>	<b>UV</b>	<b>OP</b>	<b>ST</b>
$P_i$	2.4	1.3	1.0	1.0	0.8	0.8	0.8	0.7	0.7	0.5
Rank	1	2	3	3	4	4	4	5	5	6
Ratings	I	I	PI	PI	PI	PI	PI	LI	LI	LI

#### 4.6.3 Validation and accuracy of PRAHP results











This section introduces the combination of the results obtained through PRAHP, which have been validated by selected customer comments on the respective websites where customers were dissatisfied with the trustworthiness of the website.

##### (a) Consensus results validated by consumer comments

This section shows the final fused ratings of the two techniques, i.e. the AHP and PR techniques, which rate the website in terms of its trustworthiness using the following statuses: trustworthy, untrustworthy or partially trustworthy. The trustworthiness status of websites GH to YZ is depicted in **Table 39**; website YZ is the only website that is fully trustworthy.

The AHP rating that resulted in red status, coupled with a least important website PR rating, yielded an untrustworthy website rating. The customer comments on such websites confirm customer concerns about the trustworthiness of the website.

**Table 39: Final PRAHP website ratings**

Website Name	PRAHP Results				Status	Consumer Validation Comments
GH	AHP(Amber)	+	PR(PI)	=Partially trustworthy		None≈ Trustworthy
IJ	AHP(Red)	+	PR(PI)	=Untrustworthy		I ordered a Bluetooth handset 3 years ago which I never received and I never got my refund
KL	AHP(Amber)	+	PR(PI)	=Partially trustworthy		None≈ Trustworthy
MN	AHP(Green)	+	PR(PI)	=Partially trustworthy		None≈ Trustworthy
OP	AHP(Red)	+	PR(LI)	=Untrustworthy		Customer support is very poor on this site; I have been trying to contact one of the sellers for months now and there was no success.
QR	AHP(Amber)	+	PR(PI)	=Partially trustworthy		None≈ Trustworthy
ST	AHP(Amber)	+	PR(LI)	=Untrustworthy		It appears account has been hacked and I am getting notifications of things I never bought
UV	AHP(Amber)	+	PR(LI)	=Untrustworthy		This site is careless. Some of their sellers are cheats
WX	AHP(Amber)	+	PR(I)	=Partially trustworthy		None≈ Trustworthy
YZ	AHP(Green)	+	PR(I)	=Trustworthy		None= Trustworthy

Status results in **Table 39** are accurate and based on these results it is evident that websites IJ, OP, ST and UV, which have a red rating, are classified as untrustworthy for transacting purposes.

Website YZ is the most trustworthy website, according to PRAHP. Based on the PRAHP results, it is clear that 40% of the websites were found to be completely untrustworthy, which corresponds with the complaints lodged by customers about those particular websites. The sites that are partially trustworthy made up 50% of the statistics, and only 10% were found to be fully trustworthy. These results demonstrate the reliability of the PRAHP results in providing assurance on B2B and B2C e-commerce with confidence.

#### 4.6.4 How robust is the developed PRAHP?

##### (a) Testing robustness of PRAHP through the effects of varied inbound links

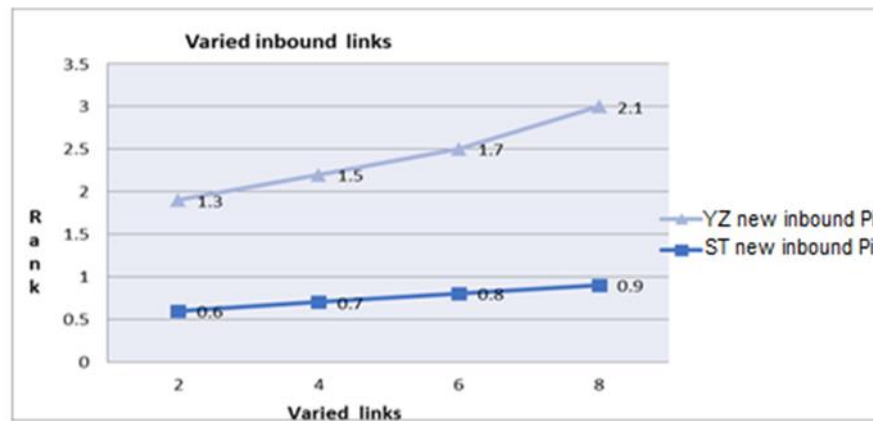
Many PR applications use the number of web links as a primary measure for website ranking. This is due to the fact that most applications are sensitive to the number of links, as these could affect the website rating. Based on PRAHP, the number of links is the determining factor for the degree of PR propagation on PRAHP from one PR to another.

The PR is often iterated between 0 and 1. The aim of this section is to confirm the hypothesis when the inbound links are adjusted in order to determine their impact.

**H<sub>0</sub>:** A rise in inbound links for a web page does not increase that page's Page rank.

**H<sub>1</sub>:** A rise in inbound links for a web page increases that page's Page rank.

**Figure 28** shows the new  $P_i$  values of the B2C website YZ and website ST as responses to the adjustment of inbound links.



**Figure 28: Varied inbound links for website YZ and ST**

Based on the results, it is evident that as the links increase, the website ranks increase. This implies that  $H_1$  is accepted and  $H_0$  rejected.

## 4.7 CHAPTER SUMMARY

This chapter looked at the trustworthiness issues on the existing e-commerce assurance models; these were discussed in section 4.2. The various assurance paradigms were also discussed in order to determine commonalities of various e-commerce assurance models. Based on the weaknesses of the existing e-commerce assurance models, a framework was proposed for e-commerce assurance, called PRAHP.

PRAHP was tested on various experiments for security, reliability, effectiveness and robustness. Ten e-commerce sites were selected for each experiment. An experiment for general e-commerce websites was done to focus on large and small e-commerce sites, as discussed in section 4.3. Based on the results of the evaluations, including the varied inbound links and varied damping factors, PRAHP proved to be robust and reliable.

Further experiments were conducted through PRAHP on cloud-based environments, as explained in section 4.4 and 4.5. The last experiment on PRAHP was done on the B2C and B2B e-commerce environment (Section 4.6) and based on these experiments; PRAHP has proven to be a consistently reliable, robust and secure method of providing e-commerce assurance.

Future research needs to focus on various e-commerce assurance issues. These have been identified and grouped by year of publication and also by the type of e-commerce topic they refer to. These issues can guide future researchers on the topics they might need to consider.

Based on the application of PRAHP on different experiments involving various e-commerce assurance markets, it is evident that PRAHP is a model that can be used in different E-commerce environments regardless of size, type and nature of the e-commerce setup. PRAHP has shown consistent and reliable results when tested on B2B, B2C and cloud-based e-commerce models, which proves the reliability of the model.



# **CHAPTER 5: OPEN E-COMMERCE ASSURANCE RESEARCH**

## **5.1 INTRODUCTION**

In order to uncover hidden e-commerce topics to assist prospective future researchers, a survey of such topics was conducted. A survey and learning structure for electronic commerce assurance was mapped, which reveals hidden topics that are less investigated.

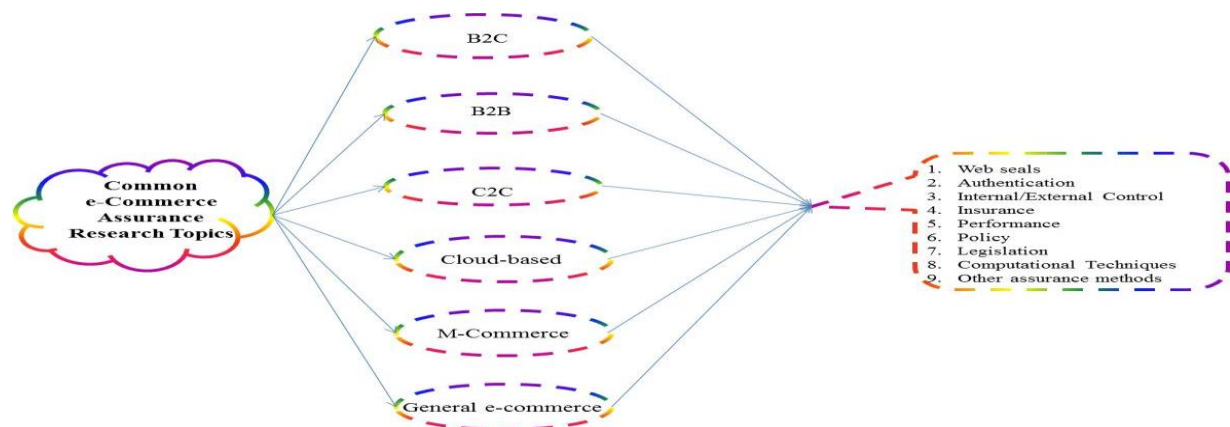
## **5.2 IMPLEMENTATION**

E-commerce assurance is speedily tightening the security facets of cyber enterprises and organisations. The assurance is being examined and integrated into almost all e-commerce businesses, which have seriously invested in security infrastructure for the success of their businesses generally. In various e-commerce segments there is increasing interest in the use of assurance as a security measure to guide online business transactions.

The internet/cyber world creates a convenient platform for buyers and sellers to transact. However, certain risks need to be mitigated, such as the security and privacy of personal information to promote online consumer trust. As e-commerce advances with the introduction of cloud computing, risks pertaining to unauthorised access and infrastructure failure need to be addressed [124]. The main research question asked is to what extent a learning structure of e-commerce assurance can be developed for revealing hidden ICT topics, which are less investigated.

This review was based mostly on a study of journals; few (less than 10%) conference proceeding papers, master's dissertations, doctoral theses, textbooks and unpublished articles were used. One expects journals to contain high-quality research information, which practitioners and academics use for disseminating assurance knowledge. When selecting a sampling frame for the literature search in January 2014, some of the following descriptors were used: "B2C", "C2C", "e-commerce assurance", "cloud-based assurance", and "mobile e-commerce assurance". The full text of every article was reviewed and selection was based on relevance to the subject of this study and the underlying research question.

The survey of literature found 149 articles published in 11 selected journals as possible publication outlets for assurance research. The research approach is subjective, since there could have been other articles on these topics that were never published or articles could have been published in languages other than English. Although this search was not exhaustive, it serves as a comprehensive base for an understanding of e-commerce assurance research, which led to the development of the learning structure shown in **Figure 30**. The starting search date was chosen as 1999, when assurance output was very low. Since the publications started picking up afterwards, the researcher therefore considered that year as the period when e-commerce assurance was gaining popularity. It was observed that previous research efforts had not classified the publishing outlets for assurance research, but 11 journals were selected based on their relevance to this research, namely: (i) Electronic commerce and research applications, (ii) Decision support systems, (iii) Government information quarterly, (iv) Information and management, (v) Industrial marketing management, (vi) Future generation computer systems, (vii) Computer law and security review, (viii) The International Journal of Management Science, (ix) Procedia Engineering, (x) Computer and Security, and (xi) Communications of the ACM.

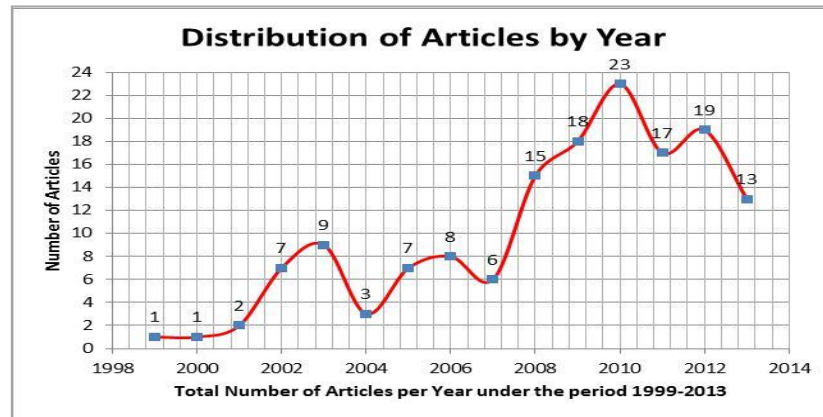


**Figure 29: Framework of open e-commerce assurance research**

In total 149 articles were classified according to the chosen scheme. The articles were identified by year of publication and the pattern of the total number of articles in the selected journal, and articles were examined by topics.

### 5.3 PATTERN OF ARTICLES BY YEAR OF PUBLICATION

The pattern of articles published by year is shown in **Figure 30** from 1999 to 2013. There seems to be limited research outputs before 2002 but the number of journal articles showed a consistent increase afterwards.



**Figure 30: Distribution of articles by year**

### 5.4 PATTERN OF ASSURANCE ARTICLES BY JOURNALS

**Figure 31** shows that the *Electronic Commerce Research and Applications* journal has by far the most articles related to e-commerce assurance topics. It publishes open access journals specifically devoted to creating and disseminating enduring knowledge for the fast-changing e-commerce environment. *Decision Support Systems* (DSS) and the *Government Information Quarterly* have the second and third largest percentage of e-commerce assurance articles. DSS, a publication of Elsevier, is dedicated to advancing concepts, techniques, evaluation and experiences of DSS, while the *Government Information Quarterly* is a journal devoted to research about IT, management, policies and practices. It focuses primarily on how policies affect government information flows and the availability/impact of IT on government innovation.

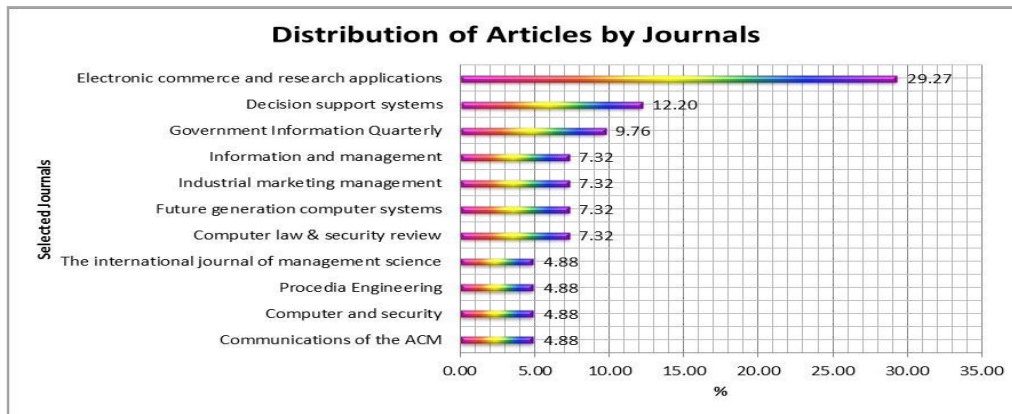


Figure 31: Pattern of assurance articles by journals

## 5.5 PATTERN OF E-COMMERCE ASSURANCE ARTICLES BY TOPICS

Figure 32 shows the distribution of articles by topics. The research topic published most frequently is B2C assurance (76 articles, 23%), while the one published least frequently is B2B assurance (37 articles, 11%).

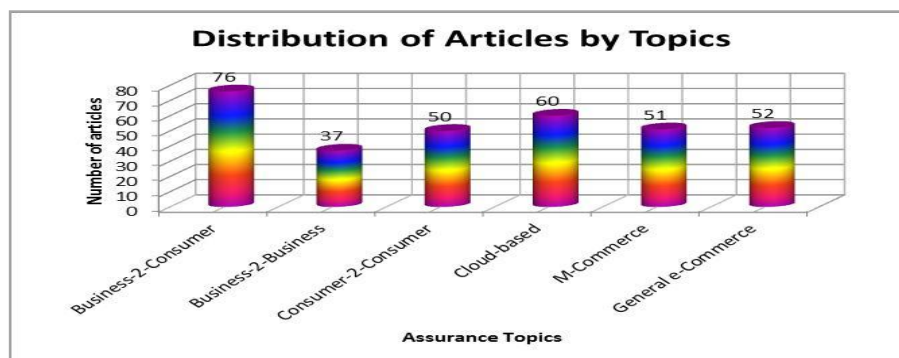


Figure 32: Pattern of assurance articles by topics

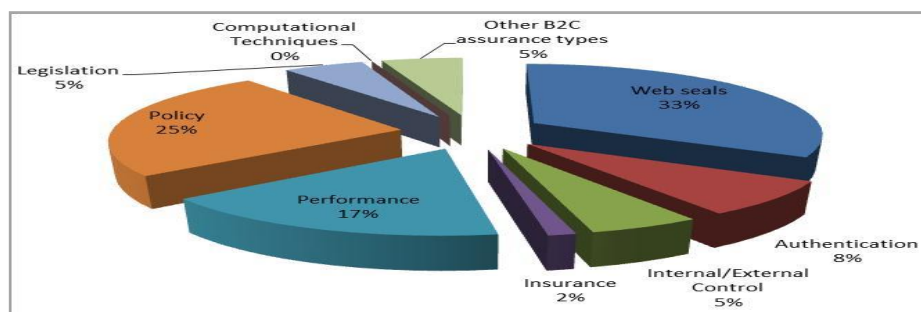
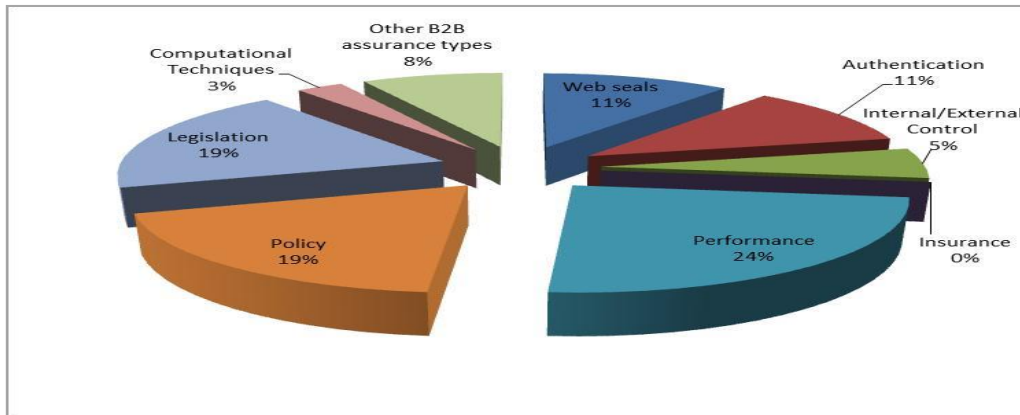


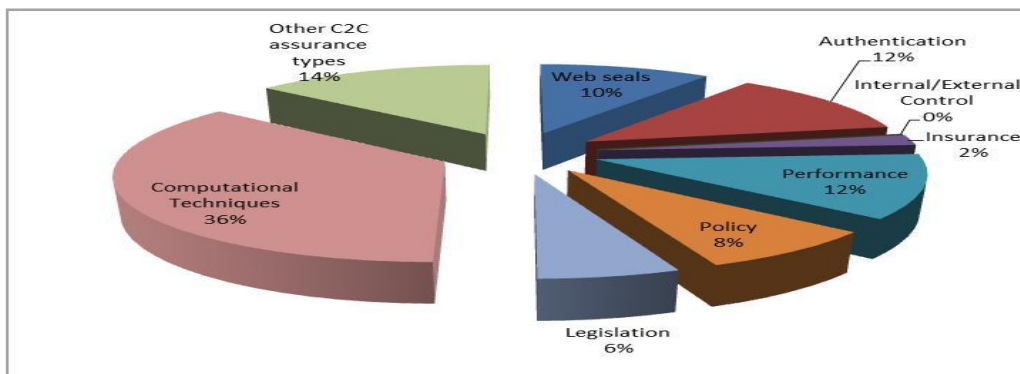
Figure 33: Number of B2C assurance articles

Figure 33 shows the percentage of articles in each B2C assurance, which is classified into nine areas. One can see that 33% of B2C articles are based on web seals and this is followed

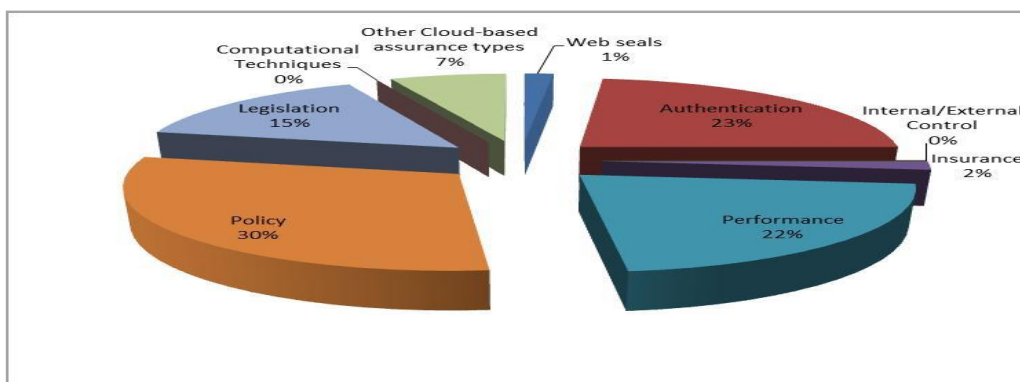
by topics on policy, 25%. **Figure 34** shows the percentage of articles on B2B assurance topics; 24% of the articles were on performance as assurance, followed by 19% related to legislation and policy.



**Figure 34: Number of B2B assurance articles**



**Figure 35: Number of C2C assurance articles**

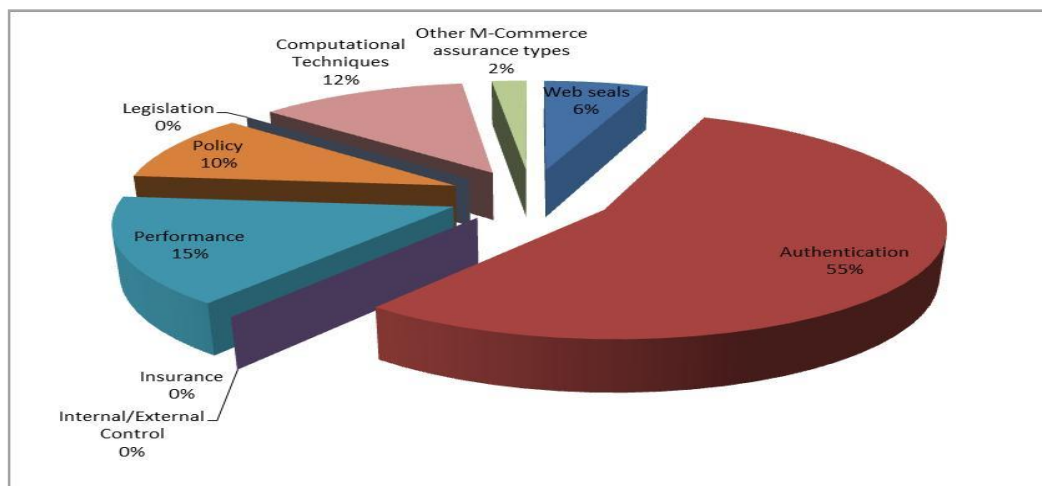


**Figure 36: Number of cloud-based articles**

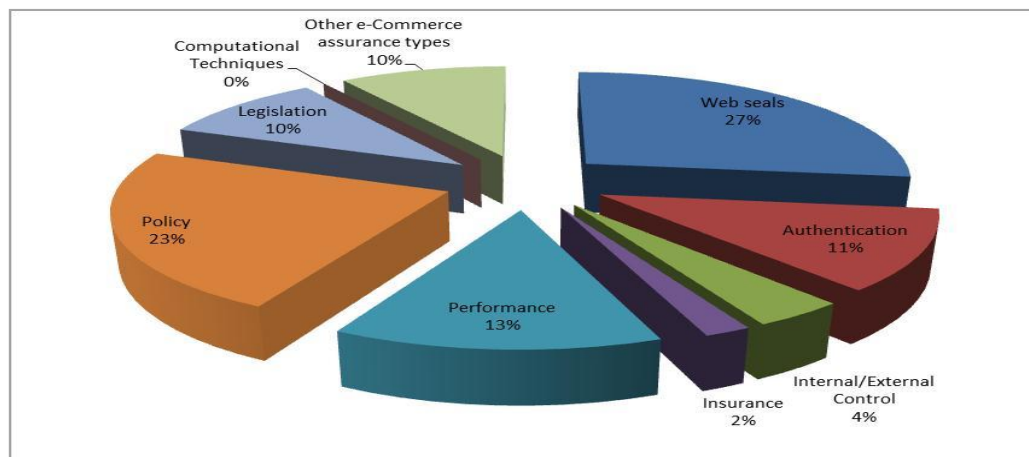
**Figure 35** shows the percentage of articles on topics related to C2C assurance: 36% of the articles were on computational techniques while 14% of the articles were related to other C2C assurance types. **Figure 36** shows the percentage of articles on topics related to cloud-

based assurance: 30% of the articles were on policy, while 23% of the articles were related to authentication.

**Figure 37** shows the percentage of articles on topics related to mobile-commerce assurance: 55% of the articles were on authentication, while 15% of the articles were related to performance. **Figure 38** shows the percentage of articles on topics related to general e-commerce assurance: 27% of the articles were on web seals, while 23% of the articles were related to policy.



**Figure 37: Number of m-commerce articles**



**Figure 38: Number of general e-commerce articles**

Future research should look at expanding the scope of the assurance attributes for inclusion in the e-commerce assurance model. Attributes such as insurance and privacy should be considered for inclusion to determine the impact thereof in providing trustworthiness. The model should also be tested on different e-commerce market types, such as mobile

application environments. Different website types should also be used, other than the ones used in this study.

## **5.6 OPEN RESEARCH QUESTIONS**

In view of the revelations on categories with no or few articles, the following are potential main research questions for future academics/researchers:

- To what extent are e-commerce assurance researchers' perceptions of the need for online business insurance explained by their years of security experience, B2C or B2B e-commerce specialisation, and intelligence-related degree?
- Does the level of e-commerce assurance among C2C customers differ based on their gender, online acquaintance, and status of business experience, after considering internal/external control and legislation?
- To what extent does a combination of web seals and internal/external control and insurance predict cloud-based assurance among e-commerce customers using computational models?
- Are rates of e-commerce crime lower in the M-commerce space when tougher legislation is applied, including internal/external controls, sophisticated web seals and insurance, when assessing online business transactions?

## **5.7. COMPARATIVE EVALUATIONS OF E-COMMERCE ASSURANCE MODELS**

This section discusses the comparison of PRAHP with other similar models. The comparison was done based on different criteria, which are discussed in subsequent sections. **Table 40** shows a comparison of PRAHP with three other assurance models based on the presence of the incorporation of the following attributes in the model: P, AS, AL, ISO compliance, availability, intelligent assurance computation and assurance level indicator. The results of the comparison show that the PRAHP has all those attributes in satisfactory measure when compared to similar models.

**Table 40: Comparative evaluation of the proposed e-commerce assurance model and related e-commerce assurance models**

Criteria	WebTrust [49][125]	COMODO Hacker proof [34]	VeriSign [126]	Proposed model
1. Policy	a) Considered b) Privacy policy	None	None	a) Considered b) Privacy policy c) Refund policy
2. Advanced security login	a) Considered b) Encryption	a)None b)Website vulnerability scan	a)None b)Encryption	a) Considered b) User login with two authentication levels c) Transaction encryption
3. Legislation	a) Considered b) Manual compliance check to privacy laws	None	None	a) Considered b) Automated compliance check to e-commerce-related legislation
4. ISO compliance	a) None	a)None	a)None	a) Considered b) Conformance check to the ISO standard 27001
5. Availability	a) Considered b) Availability regarded as an information security principle	a)None	a)None	a) Considered b) Automated availability scan
6. Intelligent assurance computation	a) None	a)None	a)None	a) Considered b) Co-operative rating based on AHP and PR techniques
7. Assurance level indicator	a) None	a)None	a)None	a) Considered b) Red Green Amber

Some of the enhancements on the PRAHP regarding the incorporation of attributes such as policy and adaptive legislation are explained in the subsequent sections (a) to (c).

#### **(a) Assurance model based on policy**

Policy – In terms of the South African ECT Act, an online vendor must have certain policies written and displayed on its website, stating the steps it will take to refund money due to certain customers and to safeguard personal information. In different existing e-commerce assurance models, policies are a simple feature, which at times users are not even aware of.



The proposed model aims to ensure that the online vendor displays an up-to-date policy statement and that the customer is made aware of the existence of the policy. It is clear that the proposed model considers more policy attributes than the existing state-of-the-art models.

#### **(b) Assurance model based on adaptive legislation**

Legislation is important in providing e-commerce assurance because it overarches self-regulation efforts. In certain web assurance models, legislation is complied with to a certain extent; however, there is no active monitoring of the online vendor site to ensure compliance. Cooperative rating will include an online check to verify whether certain information is displayed on the website, such as the company's full details, including contact information. All the results of these checks will be included in a co-operative rating. One can see that the proposed model considers more robust legislation than others do.

#### **(c) Assurance model based on intelligent assurance computation**

Many e-commerce assurance models provide static assurances, which only change over time regardless of the changing risk factors in the e-commerce space. The proposed model is aimed at creating a significant improvement on the existing e-commerce assurance models by providing intelligent assurance computation, which will show the changing status of the website's level of trustworthiness, depending on the status of controls in place for that particular website.

For instance, when a website is safe to transact from, a user will be able to tell this by the green colour display on the website and when it is unsafe it will display a red indicator. The proposed model will intelligently assess and cooperatively rate the website's level of trustworthiness, which will provide the customer with the online real-time status of the website's level of trustworthiness. This feature is unique to this model, which makes the model a significant improvement on existing e-commerce assurance models.

#### **5.7.1. Comparing PRAHP with classical approaches**

Another comparison of PRAHP was conducted based on the following criteria: level of security and reliability, reproducibility, data used, model techniques and robustness. The results of the comparison with other classical approaches are shown in **Table 41**.

Based on the assurance criteria set to assess each assurance method, it is quite evident from the results that although method 3 has certain strengths compared to methods 1 and 2, PRAHP is better than all three methods with regard to the aspects shown in **Table 41**.

**Table 41: Comparative analysis of the PRAHP assurance model and other assurance methods**

Criteria for comparison	Model 1: Monitoring assurance tools [127]	Model 2: Policies [19]	Model 3: Cloud web seals[128]	Proposed PRAHP
Security	Yes	Statements on security measures are covered	Yes. Through a series of checks performed on the website	Comprehensive security based on ISO 27001 requirements and cooperative requirements
Data inputs	Yes	No	Real website data	Objectively extracts real life data from websites
Reproducibility	None	No	No	Contains descriptive algorithms
Model technique	Online scanning	no	Online scanning	Computational PR and AHP
Robustness	Different statistics are reported based on data changes	No. Static	Different statistics are reported based on data changes	Robustness reflected on 10 websites and both validations on consumers and inbound link tests

### 5.7.2 An evaluation of PRAHP with other similar approaches

**Table 42** shows the strengths and weaknesses of assurance models in comparison with PRAHP. Based on the featured criteria in **Table 42**, it is evident that PRAHP is more robust and intelligent compared to the other three models.

**Table 42: Comparative analysis of PRAHP assurance features and other assurance methods**

Method	Strengths	Weaknesses
Static assurance - Policies [65]	It is a common assurance method in many e-commerce websites	<ul style="list-style-type: none"> <li>• When outdated and manual revision is required</li> <li>• No real-life data inputs</li> <li>• It is not a very practical assurance method, as most users cannot read the statements</li> </ul>
Third-party seals [129]	Technical assurance reviews are performed	<ul style="list-style-type: none"> <li>• Not very reliable, as seals can be forged or copied</li> <li>• Not all seals are secured</li> <li>• They provide assurance on limited, if not single, assurance attributes</li> <li>• Customer feedback not often included</li> </ul>
Monitoring tools [56]	Online checks on website details and real-life data inputs are considered	<ul style="list-style-type: none"> <li>• Assurance in the form of security is not provided</li> <li>• No transparency on the trust attributes being assessed.</li> </ul>
PRAHP	<ul style="list-style-type: none"> <li>• It uses connective intelligence of AHP and PR techniques</li> <li>• Data inputs are real-life</li> <li>• It is adaptive to accommodate changes on assurance attributes</li> <li>• It provides assurance on multiple attributes</li> <li>• It unveils the black box processes of other matters</li> <li>• Assurance accuracy readily compares with consumers' comments</li> </ul>	Probably the iterative process to correct solution

# CHAPTER 6: CONCLUSION AND FUTURE DIRECTIONS

## 6.1 OVERVIEW OF THE STUDY/RESEARCH SUMMARY

**The main research objective of this study was to develop an intelligent e-commerce assurance framework that will promote trustworthiness in online market environments.** This was accomplished in sections 3.5 and 3.6 of this research. This research objective has been accomplished through the proposed e-commerce assurance model (PRAHP). The design of the model takes into account a combination of unique techniques, AHP and PR, which are backed up by customer validation. In order to confirm the reliability of the proposed model, experiments were conducted in different e-commerce environments, i.e. B2B, B2C and cloud-based e-commerce environments. The experiments that were conducted, as explained in chapter 4, have shown that the model can be used to promote trust in e-commerce environments. The main research objective was underpinned by the following research sub-objectives:

**To develop a reliable method of identifying e-commerce assurance model attributes as important compliance measures for e-commerce sites.** This objective was reached in section 4.2.4 through the survey that was conducted to identify specific e-commerce assurance model attributes [130][131]

**To demonstrate the effectiveness of the intelligent framework in addressing security incidents in general e-commerce and on cloud-based platforms.** These demonstrations by the framework are necessary to reveal the robustness of the framework in different spheres of e-commerce when implemented. This objective was reached in sections 4.5 and 4.6, when PRAHP was tested in experiments on B2B, B2C e-commerce environments and the cloud-based environment [132][133].

**To determine if control of weaknesses of the existing assurance models and third-party seals improves the level of security through the use of the framework, specifically on B2B and B2C e-commerce sites.** The weaknesses of the existing e-commerce assurance models and third parties must be addressed in a way that will prove to be an enhancement by the proposed framework. This objective was reached in sections 4.2 and 4.6, when the proposed model was tested on the B2B and B2C e-commerce sites [134].

**To design a way to generate a comprehensive roadmap for e-commerce assurance research types for future research by academics and practitioners.** This is done to facilitate the identification of other important e-commerce assurance issues, which were not covered by this research but still needed further investigation. This objective was reached in section 4.7 through the survey that was conducted to identify e-commerce assurance hidden topics for the different e-commerce market types [135].

## **6.2 RESOLUTIONS TO RESEARCH QUESTIONS**

### **Main research question**

How can an intelligent framework of e-commerce assurances be developed to alleviate insecurity and promote trustworthiness in online market environments?

The model addressed this research by using a combination of powerful and robust techniques of AHP and PR, coupled with the inclusion of security attributes and information security best practice standards. The model is intelligent by design, as it incorporates important assurance attributes, which are supported by customer inputs. The model is versatile in that it can be used on traditional e-commerce websites and cloud-based e-commerce websites.

### **Secondary research questions:**

- How can the necessary assurance model attributes be identified to determine the level of compliance of e-commerce sites in the cyber world?

This research question has been answered through the literature survey, which singled out the important assurance attributes that are essential for inclusion in e-commerce assurance models, as discussed in section 4.2.3.

- To what extent can the framework address the widespread occurrence of insecurity, such as credit card vulnerability, unavailability of cloud services and data insecurity, in cloud-based e-commerce?

This has been addressed by testing PRAHP on various e-commerce environments, such as cloud-based environments, to confirm the reliability and robustness of the model. In addition, PRAHP was evaluated based on set criteria for some of the security attributes.

The results of the comparison, as shown in Section 5.7.2, **Table 42**, revealed that PRAHP can be used to address the widespread occurrence of security incidents and unavailability of cloud services and data insecurity.

- Does the level of information security on B2B and B2C e-commerce sites improve through the use of the framework after controlling weaknesses of assurance models and third-party security seals?

PRAHP as a model has security embedded by design, since security entails compliance with legislation, availability and best practice standards. The framework addresses most of the weaknesses of the existing assurance models to a great extent, which in turn improves the level of security in an e-commerce environment.

- How can a comprehensive roadmap for e-commerce assurance research types be investigated and structured to generate knowledge for both future academics and practitioners to safeguard online business and customers?

A review of e-commerce literature, which was done as part of this research, focusing on various e-commerce markets, was conducted as explained in sections 5.1 to 5.6. This resulted in a proper roadmap, which future researchers and practitioners can use to further their research interests.

## **6.3 SUMMARY OF CONTRIBUTIONS**

### **6.3.1 Theoretical contributions**

The study has made a significant contribution through the use of the existing literature to identify key attributes that are worth including in a robust e-commerce assurance model. These attributes were identified and discussed in sections 3.5.1.1-3.5.1.5.

A proper survey was conducted to validate the selection of these attributes, which demonstrates the unbiased view of the researcher in the selection of such attributes. This makes a significant contribution even to the work of further researchers, who may want to build on the existing attributes that have been identified for the purposes of this study.

In addition, the literature that was reviewed enabled the identification and grouping of existing e-commerce assurance weaknesses that needed to be addressed. This gives future researchers the opportunity to address those weaknesses in their quest for making a difference in the field of e-commerce.

The PRAHP, as shown in **Figure 19**, can be used by online customers, online vendors and also law enforcers to check for compliance with standards and legislation by online vendors. The model will aid online customers in making informed decisions on online purchasing, as shown in **Figures 16 and 17**. Online vendors can use the model to monitor the state of health of websites. The model will also be beneficial to law enforcers who seek to conduct checks on compliance with legislation by online stores.

Some of the proposed model's benefits are:

- It factors in legislation and standards relating to e-commerce.
- It is not a black box, as consumer inputs are required to compute the overall website rating of trustworthiness.
- It is not static, but rather provides up-to-date information to a user to make an informed purchasing decision.
- It is comprehensive and interactive in that it assesses compliance with legislation and also does online checking of technological compliance in terms of checking for the latest anti-virus software and website availability.
- It is interactive and visible through the colour display on the website.
- A dashboard (RAG) is provided as a result of a cooperative rating, which strengthens the assurance level.

### **6.3.2 Methodological contributions**

The methodology used in this research study was systematic in the sense that right from the start, a structured approach of identifying the issues in the form of weaknesses and the impact of cybercrime was done. This is covered in the investigative results, which demonstrate the weaknesses of the third-party assurance method, as shown in section 2.2.6.

The methodology of this study incorporated the use of different, yet complementary, techniques, i.e. the AHP and the PR techniques. This, coupled with customer validations, provides a strong and reliable assurance method, which has stood the test of reliability through adjusting the links and also the damping factor.

The fact that the methodology incorporated mathematical systematic computations, backed up by customer input, makes it robust and intelligent to provide the necessary information for consumer decision-making adequately.

A significant contribution of the model is its ability to calculate e-commerce assurance trustworthiness ratings using cooperative techniques. Another contribution of this model is its ability to intelligently provide more robust assurance than the ‘black box’ of web seals. Customers can safely input their credit card information on websites and safely transact. It is evident that this model has addressed all of the concerns mentioned in section 1.4.

One of the main novelties making this research relevant world-wide is an attempt to address cloud risks, which are one of the global e-commerce issues.

Some of the methodological contributions of the study include:

- An investigation on trustworthiness safety inspections and knowledge generation as a reference guide to understand e-commerce trustworthiness in general and e-commerce assurance models in particular detail for B2B, B2C and cloud-based e-commerce environments.
- Experimental evaluations of the proposed assurance model conducted on cloud-based e-commerce sites using real-life datasets.



- This research develops a new methodology, which is applied to address societal problems intended to have a socio-economic impact.

### 6.3.3 Conclusions on the empirical study

Various transactional risks are present in B2C, B2B and cloud-based e-commerce markets, which leave many customers vulnerable to online attacks. Although measures have been put in place to create trustworthy transacting platforms, comprehensive measures are still needed to give assurance on those platforms. The purpose of this study was to identify the threats and potential risks in the e-commerce markets and propose a complementary assurance model. This will assist customers to avoid transacting from risky websites.

This was achieved by examining the existing e-commerce assurance models with the aim of identifying gaps and addressing those gaps by proposing an advanced e-commerce assurance model for trustworthiness.

The gaps that were identified were grouped into the following attributes, which formed the basis of improvement on the existing e-commerce assurance model: policy, legislation, ISO standards and AS. In the proposed e-commerce assurance model, AHP and PR techniques are used to achieve cooperative ranking of the attributes, which will be displayed on the website for customer guidance regarding the website's trustworthiness, as shown in **Figures 16** and **17**. These techniques are meant to supplement each other, where the AHP process is aimed at providing a hierarchical arrangement of the attributes and assessment of the website's attributes through pairwise comparison, as discussed in sections 4.4.3, 4.5.3 and 4.6.2. These assessments were fused to come up with the final website ratings, which were validated by real-life customer comments, as shown in **Table 17** and **Table 28**.

The entire AHP and PR processes, as depicted in **Figure 15**, seek to identify those core attributes that need to be taken into account when determining the website's trustworthiness. It outlines the overall objective of the model and separates the respective attributes that ought to be assessed in order to reach a conclusion, in this case a rating. AHP is effective in the analysis of attributes or factors, since it enables the objective evaluation of the identified attributes.

Lastly, this study aims to analyse and aggregate multiple attributes, as illustrated in the various e-commerce experiments explained in Chapter 4. In order to determine the trustworthiness level of a website, it is of the utmost importance to ensure that when changes in attributes occur, the model is adjusted accordingly. Changes to legislation and revision of the ISO standards are likely to occur after a certain period and the model needs to be updated to take into account revisions in order to remain useful and reliable. The main improvement in the proposed model is to have an intelligent assurance rating, which the existing e-commerce assurance models do not have. This way of providing constant assurance to online customers will ensure that the customers remain informed on the level of trustworthiness of a website.

Specific experiments have been conducted on B2B, B2C, general e-commerce environments and cloud-based e-commerce environments, as discussed in sections 4.2-4.6, to test the reliability of PRAHP.

In testing the model to determine if it can provide reliable assurance, PRAHP provided security assurance for the private and public cloud-based e-commerce environments, as shown in **Table 28** of section 4.5.3. Experimental evaluations on both public and private cloud-based websites using the hybrid intelligent security model, as explained in section 4, revealed that the model is a reliable measure of security assurance for the sustainability of cloud-based e-commerce environments.

PRAHP was tested in the B2C and B2B e-commerce environment and the results revealed that the model was reliable. Further tests were done on PRAHP in the form of varying the damping factor to see the impact of this on the website ranking. In section 4.5.4 (**Figure 27**), the results reveal that as the damping factor increases for e-commerce websites, the website rank's propagation tends to be distributed, which shows the reliability of PRAHP for trustworthiness assurance.

PRAHP's reliability was also tested by varying the inbound links. As illustrated in experiments discussed in sections 4.6.4 and 4.5.4 for B2C and cloud-based e-commerce websites, it is evident that PRAHP is reliable in providing e-commerce assurance. This is illustrated by the fact that as the number of links increases, both website ranks increase, which suggests that  $H_0$  is rejected and  $H_1$  is accepted.

## **6.4 RECOMMENDATIONS**

Based on the results of this study, it is evident that various e-commerce stores or markets at large stand to benefit from the use of PRAHP. For business organisations on B2B, the use of PRAHP can make parties trust each other when it is used in their environment as a model for assuring parties of the trustworthiness of such platforms. The researcher recommends this tool to B2B e-commerce stores to ensure that every party to the transaction is trustworthy.

PRAHP is useful in B2C e-commerce environments, where customers will not easily fall prey to scams or transacting from fictitious sites. The use of PRAHP by B2C e-commerce markets will position the stores in a trustworthy manner, since users will be able to make purchasing decisions based on the assurance level they receive from PRAHP.

CSPs and consumers alike can benefit from the use of PRAHP for assurance purposes in cloud-based e-commerce environments regarding the security and availability of systems, among other assurance attributes.

The researcher recommends the use of PRAHP to online stores that sell products or services, as it will be a reliable assurance measure that will help safeguard the trust relationship of all parties involved in the transaction. In terms of the work done in this research to identify open research topics on e-commerce, the researcher recommends that researchers take it a step further and investigate other elements that need to be incorporated.

Legal experts and law enforcement centres in various countries should consider the use of PRAHP in enforcing compliance with legislation and where possible, compliance to some of the best practice standards.

## **6.5 LIMITATIONS AND FUTURE DIRECTIONS**

### **(a) Theoretical limitations**

Literature on e-commerce assurance was quite limited at the time the study was conducted and in certain instances literature dating back to 1999 had to be consulted to identify some of the trends. This had an impact on the limitation of assurance attributes to five attributes, since those emanated from the themes in the relevant existing literature. The use of inconsistent terminology in some of the literature made it challenging to mine the relevant themes in some of the sources of literature reviewed, e.g. the use of seals of accreditation versus web seals.

Other computational techniques must be considered to build robust e-commerce assurance models.

### **(b) Methodological limitations**

The sample size of the websites used for the experiments was limited and did not include other different e-commerce markets such as customer-to-business and business-to-administration websites.

Only English websites were considered for the study and others not written in English, such as Chinese e-commerce websites, were excluded for experimental purposes. As a result a review of other assurance methods might have been omitted.

The proposed model did not cover all attributes that are present in various e-commerce environments, e.g. G2C; future research work should also investigate assurance attributes such as privacy that can be included as part of the model to provide comprehensive assurance of a website.

The scope of assurance models should be extended to mobile applications, since most e-commerce stores have mobile applications that enable electronic purchasing.

### **(c) Future directions**

Future researchers should focus on uncovering and researching hidden e-commerce issues. The important research articles are spread across different journals.

In the 11 selected journals that are relevant outlets for assurance research, an in-depth literature survey was conducted to find assurance-related articles. This resulted in the identification of 149 accredited journal articles published between 1999 and 2013. This outcome provides useful insights into the understanding of the assurance research structure, but cannot claim to be exhaustive.

Most results that received a little research attention consistently placed insurance and internal/external control at the top of the categories considered. These assurance measures are part of the major pillars that support e-commerce trustworthiness. It is, however, challenging to find articles on computational techniques for assessing e-commerce. Further research should address the shortcomings outlined in this section and ask some of the research questions outlined in section 5.6, i.e.:

- To what extent are e-commerce assurance researchers' perceptions of the need for online business insurance explained by their years of security experience, B2C or B2B e-commerce specialisation, and intelligence related-degree?
- Does the level of e-commerce assurance among C2C customers differ based on their gender, online acquaintance and status of business experience, after considering internal/external control and legislation?
- To what extent does a combination of web seals and internal/external control and insurance predict cloud-based assurance among e-commerce customers using computational models?
- Are rates of e-commerce crimes lower in the m-commerce space when using tougher legislation, including internal/external controls and sophisticated web seals and insurance when assessing online business transactions?

## BIBLIOGRAPHY

- [1] Tech Central, "Home Page," 2012. [Online]. Available: <http://www.techcentral.co.za/new-study-sas-internet-economy-2-of-gdp/32212/>. [Accessed: 20-Jul-2008].
- [2] E-commerce News, "Home," 2017. [Online]. Available: <https://ecommercenews.eu/ecommerce-uk-reach-e174-billion-2016/>. [Accessed: 01-Jul-2017].
- [3] Internet Retailer, "Home Page," 2017. [Online]. Available: <https://www.internetretailer.com/trends/sales/us-e-commerce-sales-2005-2015/>. [Accessed: 01-Jun-2017].
- [4] E. Mik, "Mistaken identity, identity theft and problems of remote authentication in e-commerce," *Comput. Law Secur. Rev.*, vol. 28, no. 4, pp. 396–402, 2012.
- [5] S. Alsharnouby, M. Alaca, F. Chiasson, "Why phishing still works: User strategies for combating phishing attacks," *Int. J. Hum. Comput. Stud.*, vol. 82, pp. 69–82, 2015.
- [6] S. Shekocar, N.M. Shah, C. Mahajan, M. Racch, "An ideal approach for detection and prevention of phishing attacks," *Procedia Comput. Sci.*, vol. 82, no. 49, pp. 82–91, 2015.
- [7] Alibaba, "Home Page", 2017. [Online]. Available: <http://www.alibaba.com/>. [Accessed: 01-Mar-2017].
- [8] M. A. Eastlick, S. L. Lotz, and P. Warrington, "Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment," *J. Bus. Res.*, vol. 59, no. 8, pp. 877–886, 2006.
- [9] A. D. Beldad, M. de Jong, and M. F. Steehouder, "When the bureaucrat promises to safeguard your online privacy: Dissecting the contents of privacy statements on Dutch municipal websites," *Gov. Inf. Q.*, vol. 26, no. 4, pp. 559–566, 2009.
- [10] B. Edelman, "Adverse selection in online 'trust' certifications and search results," *Electron. Commer. Res. Appl.*, vol. 10, no. 1, pp. 17–25, 2011.
- [11] C. Hooper, B. Martini, and K. K. R. Choo, "Cloud computing and its implications for cybercrime investigations in Australia," *Comput. Law Secur. Rev.*, vol. 29, no. 2, pp. 152–163, 2013.
- [12] S.M. Huang, LY. Chou, and D.-H. Shih, "Understanding the effect of third-party web assurance seals on consumers' trust, from the perspective of the seal providers," *Technol. Manag. Emerg. Technol. (PICMET), 2012 Proc. PICMET '12*, pp. 1073–

- 1078, 2012.
- [13] M. Ouedraogo and H. Mouratidis, "Selecting a cloud service provider in the age of cybercrime," *Comput. Secur.*, vol. 38, pp. 3–13, 2013.
  - [14] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," *Comput. Electr. Eng.*, vol. 39, no. 1, pp. 47–54, 2013.
  - [15] S. E. Kaplan and R. J. Nieschwietz, "A web assurance services model of trust for B2C e-commerce," *Int. J. Account. Inf. Syst.*, vol. 4, no. 2, pp. 95–114, 2003.
  - [16] T. Bahmanziari, M. D. M. Odom, and J. C. J. Ugrin, "An experimental evaluation of the effects of internal and external e-assurance on initial trust formation in B2C e-commerce," *Int. J. Account. Inf. Syst.*, vol. 10, no. 3, pp. 152–170, 2009.
  - [17] K. M. Kimery and M. Mccord, "Third-party assurances: Mapping road to trust in E-retailing," *J. Inf. Technol. Theory Appl.*, vol. 4, no. 2, pp. 63–82, 2002.
  - [18] X. Hu, G. Wu, Y. Wu, and H. Zhang, "The effects of web assurance seals on consumers' initial trust in an online vendor: A functional perspective," *Decis. Support Syst.*, vol. 48, no. 2, pp. 407–418, 2010.
  - [19] Oracle, "Home," 2016. [Online]. Available: <https://www.oracle.com/index.html>. [Accessed: 01-Jun-2016].
  - [20] Ebay, "Home," 2016. [Online]. Available: <https://www.ebay.com/>. [Accessed: 01-Jun-2016].
  - [21] Spree, "Home Page," 2017. [Online]. Available: <http://www.spree.co.za/>. [Accessed: 01-Mar-2017].
  - [22] S.Writer, "Gumtree scams: What to watch out for and how to avoid them," 2016. [Online]. Available: <https://mybroadband.co.za/news/security/174598-gumtree-scams-what-to-watch-out-for-and-how-to-avoid-them.html>. [Accessed: 09-Mar-2017].
  - [23] J.Morgan, "Simple explanations of internet of things," 2014. [Online]. Available: <https://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#5b161b061d09>. [Accessed: 30-Jun-2018].
  - [24] A.Yan, Z., Zhang, P., Vasilakos, "A survey on trust management for internet of things," *A J. Netw. Comput. Appl.*, vol. 42, p. 120–134., 2014.
  - [25] I. Bao, F.,Chen, "Trust management for the Internet of things and its application to service composition," in *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, 2012.
  - [26] A. Beldad, M. de Jong, and M. Steehouder, "How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust," *Comput. Human*

- Behav.*, vol. 26, no. 5, pp. 857–869, 2010.
- [27] C. Kim, W. Tao, N. Shin, and K. S. Kim, “An empirical study of customers’ perceptions of security and trust in e-payment systems,” *Electron. Commer. Res. Appl.*, vol. 9, no. 1, pp. 84–95, 2010.
  - [28] S. Iglesias-Pradas, F. Pascual-Miguel, Á. Hernández-García, and J. Chaparro-Peláez, “Barriers and drivers for non-shoppers in B2C e-commerce: A latent class exploratory analysis,” *Comput. Human Behav.*, vol. 29, no. 2, pp. 314–322, 2013.
  - [29] Y. Fang, I. Qureshi, H. Sun, P. McCole, E. Ramsey, and K. H. Lim, “Trust, satisfaction, and online repurchase intention: The moderating role of perceived effectiveness of e-commerce institutional mechanisms,” *MIS Q. Manag. Inf. Syst.*, vol. 38, no. 2, 2014.
  - [30] H. Zhang, Y. Wang, and X. Zhang, “Efficient contextual transaction trust computation in E-commerce environments,” in *Proc. of the 11th IEEE Int. Conference on Trust, Security and Privacy in Computing and Communications, TrustCom-2012 - 11th IEEE Int. Conference on Ubiquitous Computing and Communications, IUCC-2012*, 2012.
  - [31] A. M. Abbadi, Imad M., “Trust in the cloud,” *Inf. Secur. Tech. Rep.*, vol. 16, no. 3, pp. 108–114, 2011.
  - [32] K. Kimery and M. McCord, “Signals of trustworthiness in e-commerce: Consumer understanding of third-party assurance seals,” *J. Electron. Commer.*, 2006.
  - [33] Amazon Web Services, “Privacy.” [Online]. Available: <https://aws.amazon.com/compliance/?hp=tile>. [Accessed: 27-Jan-2017].
  - [34] Comodo, “Home Page,” 2017. [Online]. Available: <https://www.comodo.com/e-commerce/site-seals/network-vulnerability-scan.php>. [Accessed: 01-Mar-2017].
  - [35] IBM, “ISO 27001 Certifications,” *ISO 27001*. [Online]. Available: [https://www-935.ibm.com/services/us/en/it-services/iso\\_27001\\_\\_a1031826.html](https://www-935.ibm.com/services/us/en/it-services/iso_27001__a1031826.html). [Accessed: 30-Apr-2017].
  - [36] Payment Card Industry Standard, “Home Page,” 2017. [Online]. Available: [https://www.pcisecuritystandards.org/pci\\_security/](https://www.pcisecuritystandards.org/pci_security/). [Accessed: 01-Mar-2017].
  - [37] “Truste Seals,” 2017. [Online]. Available: <https://www.truste.com/business-products/trusted-websites/>. [Accessed: 23-Mar-2017].
  - [38] Trusted Cloud, “Home page,” 2015. [Online]. Available: <http://www.truste.com/business-products/trusted-cloud>. [Accessed: 01-Apr-2015].
  - [39] Volusion, “Home,” 2017. [Online]. Available: <https://www.volusion.com/>. [Accessed: 15-Aug-2017].



- [40] J. Lin and Y. Lu, "The study of consumer trust transference for the adoption of mobile service," *2009 Int. Conf. Manag. Serv. Sci.*, 2009.
- [41] J. C., C. M. Jackson, and L. Graham, "Issues and risks in performing SysTrust® engagements: Implications for research and practice," *Int. J. Account. Inf. Syst.*, vol. 6, no. 1, pp. 55–79, 2005.
- [42] N. J. Rifon, R. Larose, and S. M. Choi, "Your privacy is sealed: Effects of web privacy seals on trust and personal disclosures," *J. Consum. Aff.*, vol. 39, no. 2, pp. 339–362, 2005.
- [43] P. Loshin, "Acer's e-commerce website hit by a customer data breach," 2016. [Online]. Available: <http://searchsecurity.techtarget.com/news/450298892/Acers-ecommerce-website-hit-by-a-customer-data-breach>. [Accessed: 01-Mar-2017].
- [44] Website Privacy Certification, 2017. [Online]. Available: <https://www.european-privacy-seal.eu/EPs-en/website-privacy-certification-overview>. [Accessed: 01-Mar-2017].
- [45] Loot, "Hot deals," 2017. [Online]. Available: <http://www.loot.co.za/>. [Accessed: 01-Jan-2017].
- [46] McAfee Secure, 2017. [Online]. Available: <https://www.mcafeesecure.com/for-consumers>. [Accessed: 01-Mar-2017].
- [47] Comodo, "Home Page," 2017. [Online]. Available: <https://www.comodo.com/e-commerce/site-seals/network-vulnerability-scan.php>. [Accessed: 20-Jul-2001].
- [48] Better Business Bureau, "Home Page," 2017. [Online]. Available: <https://www.bbb.org/lexington/for-businesses/about-bbb-accreditation/for-accredited-businesses/bbb-dynamic-seal/>. [Accessed: 20-Jul-2017].
- [49] WebTrust, "Home Page." [Online]. Available: <https://cert.webtrust.org/ViewSeal?id=2058>. [Accessed: 01-Mar-2017].
- [50] Superbalist, "Home Page", 2017. [Online]. Available: <https://superbalist.com/>. [Accessed: 01-Mar-2017].
- [51] Shopify, "Home Page," [Online]. 2017. Available: <https://shopify.com/>.
- [52] Shop Goodwill, "Home Page," 2017. [Online]. Available: <https://www.shopgoodwill.com/>. [Accessed: 01-Mar-2017].
- [53] Webstore, "Home Page," 2016. [Online]. Available: <http://www.webstore.com/>. [Accessed: 20-Jun-2006].
- [54] Ticket Gateway, "Home Page" 2017. [Online]. Available: <https://www.ticketgateway.com/pages/security>. [Accessed: 01-Mar-2017].

- [55] Data secure works, "Home Page," 2017. [Online]. Available: <http://www.datasecureworks.com/>. [Accessed: 01-May-2017].
- [56] S. Advisor, "Home Page," 2017. [Online]. Available: <http://www.scamadviser.com/>. [Accessed: 01-Mar-2017].
- [57] T. Moores, "The Role of privacy seals in e-commerce," *Commun. ACM*, vol. 48, no. 3, pp. 86–91, 2005.
- [58] Better Business Bureau, "Home Page", 2017. [Online]. Available: <https://www.bbb.org/lexington/for-businesses/about-bbb-accreditation/for-accredited-businesses/bbb-dynamic-seal/>. [Accessed: 01-Mar-2017].
- [59] Thompson Travel, "Home Page", 2017. [Online]. Available: <http://thompsonstravel.co.za/>. [Accessed: 01-Mar-2017].
- [60] T. Branigan, "Alibaba.com chief executive resigns," *The Guardian*, 2011. [Online]. Available: [https://www.theguardian.com/business/2011/feb/21/alibaba-chief-resigns-over-frauds?CMP=tw\\_t\\_gu](https://www.theguardian.com/business/2011/feb/21/alibaba-chief-resigns-over-frauds?CMP=tw_t_gu). [Accessed: 09-Mar-2017].
- [61] A. Adrian, "How much privacy do clouds provide? An Australian perspective," *Comput. Law Secur. Rev.*, vol. 29, no. 1, pp. 48–57, 2013.
- [62] Gumtree, "Home Page," 2017. [Online]. Available: [www.gumtree.co.za](http://www.gumtree.co.za). [Accessed: 15-Jun-2016].
- [63] D. Gefen, "E-commerce: The role of familiarity and trust," *Omega*, vol. 28, no. 6, pp. 725–737, 2000.
- [64] B. J. Corbitt, T. Thanasankit, and H. Yi, "Trust and e-commerce: A study of consumer perceptions," *Electron. Commer. Res. Appl.*, vol. 2, no. 3, pp. 203–215, 2003.
- [65] Woolworths, "Home Page," 2017. [Online]. Available: [//www.woolworths.co.za/store/fragments/corporate/corporate-index.jsp?content=corporate-content&contentId=cmp205289](http://www.woolworths.co.za/store/fragments/corporate/corporate-index.jsp?content=corporate-content&contentId=cmp205289). [Accessed: 01-Aug-2017].
- [66] Y. Pan and G. M. Zinkhan, "Exploring the impact of online privacy disclosures on consumer trust," *J. Retail.*, vol. 82, no. 4, pp. 331–338, 2006.
- [67] Walmart, "Home Page." 2017. [Online]. Available: <https://www.walmart.com/all-departments>
- [68] Taobao, "Home Page," 2017. [Online]. Available: <http://www.engtaobao.com/guide/view/charge-policy.html>. [Accessed: 20-Jul-2001].
- [69] S. Utz, P. Kerkhof, and J. van den Bos, "Consumers rule: How consumer reviews influence perceived trustworthiness of online stores," *Electron. Commer. Res. Appl.*,

- vol. 11, no. 1, pp. 49–58, 2012.
- [70] Toppik, “Home Page.” [Online]. Available: <https://toppik.com.au/money-back-guarantee>. [Accessed: 01-Jan-2017].
  - [71] Blue Grass, “Home,” 2017. [Online]. Available: <https://bluegrass.app.bbb.org/dynamic-seal>). [Accessed: 30-Oct-2017].
  - [72] J. Zhao, S. Wang, and W. V. Huang, “A study of B2B e-market in China: E-commerce process perspective,” *Inf. Manag.*, vol. 45, no. 4, pp. 242–248, 2008.
  - [73] C. Everett, “Cloud computing - A question of trust,” *Comput. Fraud Secur.*, vol. 2009, no. 6, pp. 5–7, 2009.
  - [74] D. Data, “Home,” 2015. [Online]. Available: [www.dimensiondata.com](http://www.dimensiondata.com)%0A. [Accessed: 01-Sep-2015].
  - [75] C. Network, “Home,” 2016. [Online]. Available: [www.cloudnetwork.co.za](http://www.cloudnetwork.co.za). [Accessed: 01-Sep-2016].
  - [76] Hpe, “Home,” 2016. [Online]. Available: [www.hpe.com](http://www.hpe.com). [Accessed: 01-Sep-2016].
  - [77] Salesforce, “Home,” 2016. [Online]. Available: [www.salesforce.com](http://www.salesforce.com). [Accessed: 01-Sep-2016].
  - [78] VMWARE, “Home,” 2016. [Online]. Available: [www.vmware.com](http://www.vmware.com). [Accessed: 01-Jun-2016].
  - [79] B. Gilbert, “Sony website hacked,” 2017. [Online]. Available: <http://www.businessinsider.com/playstation-network-allegedly-hacked-ourmine-2017-8>. [Accessed: 30-Oct-2017].
  - [80] Cloud on Demand, “Cloud on demand,” 2017. [Online]. Available: <http://www.cloudondemand.co.za/privacy.aspx>.
  - [81] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, 2011.
  - [82] D. Sitaram and G. Manjunath, “Chapter 7 - Designing cloud security,” in *Moving To The Cloud*, 2012, pp. 307–328.
  - [83] N. Kshetri, “Privacy and security issues in cloud computing: The role of institutions and institutional evolution,” *Telecomm. Policy*, vol. 37, no. 4–5, pp. 372–386, 2013.
  - [84] Amazon Web Services, “AWS cloud computing services,” 2017. [Online]. Available: <https://aws.amazon.com/compliance/?hp=tile>. [Accessed: 01-Jan-2017].
  - [85] A. Devi, P., Gupta, A. and Dixit, “Comparative study of HITS and PageRank link based ranking algorithms,” *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 3, no. 2, 2014.

- [86] Wikipedia, "Home Page," 2016. [Online]. Available: <https://en.wikipedia.org/wiki/PageRank>. [Accessed: 01-Nov-2017].
- [87] Check Page Rank, "Home Page," 2017. [Online]. Available: <http://checkpagerank.net/>. [Accessed: 01-Mar-2017].
- [88] Page Rank Checker, "Home Page," 2017. [Online]. Available: <https://www.prchecker.info/>. [Accessed: 01-Mar-2017].
- [89] J. M. Kleinberg, "Authoritative sources in a hyperlinked environment," *J. ACM*, vol. 46, no. 5, pp. 604–632, 1999.
- [90] C. C. Chien, O.K., Hoong, P.K and Ho, "A comparative study of HITS vs PageRank algorithms for Twitter users analysis," *Int. Conf. Comput. Sci. Technol.*, 2014.
- [91] R. Russo, R.F.S, and Camanho, "Criteria in AHP: A Systematic review of literature," *Inf. Technol. Quant. Manag.*, vol. 55, pp. 1123 – 1132, 2015.
- [92] O. R. Breaz, and R.E. Bologa, "Selecting industrial robots for milling applications using AHP," *Inf. Technol. Quant. Manag.*, vol. 122, pp. 346–353, 2017.
- [93] J. V. J. Mimović, and P. Stanković, "Decision-making under uncertainty – The integrated approach of the AHP and Bayesian analysis," *Econ. Res. Istraživanja*, vol. 28, no. 1, 2015.
- [94] P. Beynon, M. Curry, and B. Morgan, "The Dempster-Shafer theory of evidence: Alternative approach to multicriteria decision modelling," *Int. J. Manag. Sci.*, vol. 28, pp. 37–50, 2000.
- [95] K. B. Tay and J. Chelliah, "Disintermediation of traditional chemical intermediary roles in the electronic business-to-business (e-B2B) exchange world," *J. Strateg. Inf. Syst.*, vol. 20, no. 3, pp. 217–231, 2011.
- [96] Barnard S., "AHP," *AHP tool*, 2012. [Online]. Available: <http://www.scbuk.com>. [Accessed: 01-Jan-2013].
- [97] ISO 27002, "ISO/IEC 27002," 2013. [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html>. [Accessed: 20-Jul-2016].
- [98] ISO 27001, "ISO/IEC 27001," 2013. [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html>. [Accessed: 20-Jul-2016].
- [99] Electronic Communications and Transactions Act, *Electronic communications.*, vol. 4, no. 10505. South Africa, 2002, pp. 1–4.
- [100] Bidorbuy, "Home," 2017. [Online]. Available: <https://www.bidorbuy.co.za/>. [Accessed: 01-Oct-2017].
- [101] ISO/IEC 27017:2015, "Home." [Online]. Available:

- [http://www.iso.org/iso/home/store/catalogue\\_tc/catalogue\\_detail.htm?csnumber=4375](http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=4375)  
7. [Accessed: 27-Jan-2017].
- [102] BelaBela, "ICT security policy," 2017. [Online]. Available:  
[http://www.belabela.gov.za/docs/policies/ICT Information Security Policy.pdf](http://www.belabela.gov.za/docs/policies/ICT%20Information%20Security%20Policy.pdf).  
[Accessed: 30-Apr-2017].
- [103] Fashion Hub, "Fashion Hub." [Online]. Available:  
<http://fashionhub.co.za/?gclid=CN73w53rzNMCFeYp0wodczMEjw>. [Accessed: 30-Apr-2017].
- [104] My Car, "Home Page," 2017. [Online]. Available: <https://www.mycars.co.za/>.  
[Accessed: 30-Apr-2017].
- [105] Cape Coffee Beans, "Home." [Online]. Available:  
[https://capecoffeebeans.co.za/?gclid=CPeai4\\_rsscCFSMcwwodP6UICw](https://capecoffeebeans.co.za/?gclid=CPeai4_rsscCFSMcwwodP6UICw). [Accessed:  
30-Apr-2017].
- [106] Fastenal, "Home Page," 2017. [Online]. Available:  
<https://www.fastenal.com/logon/sign-in>. [Accessed: 01-Jun-2017].
- [107] Site 24x7, "Check website availability." [Online]. Available:  
<https://www.site24x7.com/check-website-availability.html>. [Accessed: 30-Apr-2017].
- [108] Forbes, "How important are customer reviews for online marketing?," 2016. [Online].  
Available: <https://www.forbes.com/sites/jaysondemers/2015/12/28/how-important-are-customer-reviews-for-online-marketing/#937c5aa19284>. [Accessed: 01-Dec-2016].
- [109] V. K. Vamsee , M.Krishna Kiran M, R.E Vinodhini and R. Archanaa , "User specific product recommendation and rating system by performing sentiment analysis on product reviews," *International Conference on Advanced Computing and Communication Systems*, 2017, pp. 1–5.
- [110] Statistics How To, "Home Page," 2016. Available:<https://www.statisticshowto.com>
- [111] R. J. Daigle and J. C. Lampe, "The level of assurance precision and associated cost demanded when providing continuous online assurance in an environment open to assurance competition," *Int. J. Account. Inf. Syst.*, vol. 6, no. 2, pp. 129–156, 2005.
- [112] V. Lala, V. Arnold, S. G. Sutton, and L. Guan, "The impact of relative information quality of e-commerce assurance seals on internet purchasing behavior," *Int. J. Account. Inf. Syst.*, vol. 3, no. 4, pp. 237–253, 2002.
- [113] B. Runyan, K. Smith, and L. Smith, "Implications of web assurance services on e-commerce," *Account. Forum*, 2008.
- [114] I. Hosein and E. A. Whitley, "The regulation of electronic commerce: Learning from

- the UK's RIP act," *J. Strateg. Inf. Syst.*, vol. 11, no. 1, pp. 31–58, 2002.
- [115] C. A. Primo Braga, "E-commerce regulation: New game, new rules?," *Q. Rev. Econ. Financ.*, vol. 45, no. 2–3 SPEC. ISS., pp. 541–558, 2005.
- [116] M. Gerber and R. von Solms, "Information security requirements – Interpreting the legal aspects," *Comput. Secur.*, vol. 27, no. 5, pp. 124–135, 2008.
- [117] C. Liao, C.-C. Liu, and K. Chen, "Examining the impact of privacy, trust and risk perceptions beyond monetary transactions: An integrated model," *Electron. Commer. Res. Appl.*, vol. 10, no. 6, pp. 702–715, 2011.
- [118] C. H. Lee and D. A. Cranage, "Personalisation-privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel web sites," *Tour. Manag.*, vol. 32, no. 5, pp. 987–994, 2011.
- [119] A. Torrubia, F. J. Mora, and L. Marti, "Cryptography regulations for e-commerce and digital rights management," *Comput. Secur.*, vol. 20, no. 8, pp. 724–738, 2001.
- [120] E. G. Mauldin, A. I. Nicolaou, and S. E. Kovar, "The influence of scope and timing of reliability assurance in B2B e-commerce," *Int. J. Account. Inf. Syst.*, vol. 7, no. 2, pp. 115–129, 2006.
- [121] KYPLEX, "Keep your website clean from malware," 2013. [Online]. Available: <http://www.kyplex.com/security-seal.html#domain=http://www.kyplex.com/>. [Accessed: 01-Dec-2013].
- [122] A. Gray, "Conflict of laws and the cloud," *Comput. Law Secur. Rev.*, vol. 29, no. 1, pp. 58–65, 2013.
- [123] A. Neto, A.M.Ritter, L. Leite, N. Zampieri, D.E. Lotufo and R. Mendeleck, "Pearson's Correlation coefficient for discarding redundant information in real time autonomous navigation system," in *16th Int'l Conference on Control Applications*, 2007, pp. 426–431.
- [124] M. MacKay, T. Baker, and A. Al-Yasiri, "Security-oriented cloud computing platform for critical infrastructures," *Comput. Law Secur. Rev.*, vol. 28, no. 6, pp. 679–686, 2012.
- [125] Shop Bop, "Home," 2017. [Online]. Available: [www.shopbop.com](http://www.shopbop.com). [Accessed: 01-Oct-2017].
- [126] Soap, "Home," 2012. [Online]. Available: [www.soap.com](http://www.soap.com). [Accessed: 01-Nov-2012].
- [127] Qualys, "Qualys cloud platform," 2017. [Online]. Available: <https://www.qualys.com/cloud-platform/>. [Accessed: 01-Aug-2017].
- [128] Trust Guard, "Home," 2017. [Online]. Available: <https://www.trust->

- guard.com/?utm\_expid=1880506-126.6QaTq31IRN62VthELRfhJg.0&utm\_referrer=https%3A%2F%2Fwww.google.co.za%2F. [Accessed: 01-Oct-2017].
- [129] Zando, “Home Page,” 2016. [Online]. Available: [www.zando.co.za](http://www.zando.co.za). [Accessed: 01-Jun-2016].
- [130] T. Mayayise and I. Osunmakinde, “A compliant assurance model for assessing the trustworthiness of cloud-based e-commerce systems,” *2013 Inf. Secur. South Africa - Proc. ISSA 2013 Conf.*, 2013.
- [131] T. Mayayise and I. O. Osunmakinde, “E-commerce assurance models and trustworthiness issues: An empirical study,” *Inf. Manag. Comput. Secur.*, vol. 22, no. 1, pp. 76–96, 2014.
- [132] T. Mayayise and I. O. Osunmakinde, “Intelligent Hybrid Security Model for a Safer Cloud-based e-commerce,” *Kasmera J.*, vol. 44, no. 1, 2016.
- [133] T. O. Mayayise and I. O. Osunmakinde, “Robustness of computational intelligent assurance models when assessing e-Commerce sites,” in *2015 Information Security for South Africa - Proceedings of the ISSA 2015 Conference*, 2015.
- [134] T. Mayayise, and I. O. Osunmakinde, “Connective intelligence to stay safe while Shopping online for E-products and E-services on business-2-business and business-2-consumer websites,” *Int. J. Bus. Inf. Syst.*, 2017.
- [135] I. O. Osunmakinde, and T. O. Mayayise, “A learning structure of E-commerce assurance revealing hidden ICT topics in cyber world,” in *ICT Education in the Cyber World*, 2014.